Resilience Engineering Association

7th REA Symposium

LIÈGE université

Poised to Adapt: Enacting resilience potential through design, governance and organization

Proceedings

EDITED BY
Anne-Sophie Nyssen
Mathieu Jaspar
David Woods

26th – 29th June 2017
Liège – Comtes de Méan
www.rea-symposium.org/

Preface

Poised to Adapt: Enacting resilience potential through design, governance and organization

In a world of changing pressures, relationships, interdependencies, and possibilities, past performance and safety records, however successful, need to be adapted and new approaches innovated. A key is the ability to continuously anticipate and adapt to keep pace with change. But what does it mean for teams and organizations to be poised to adapt as tempos of change vary?

Today's organizations focus on ensuring compliance to a model of success embodied in plans, procedures, quality indicators, and automation. The assumption is that the model of success already accounts for uncertainties and minimizes the unexpected. This assumption fails in our interconnected and turbulent world. Compliance oriented systems are very brittle when facing unexpected events and changes.They experience surprising, sudden collapses in performance, such as dramatic service outages, occur regularly despite a backdrop of improving scores on indicators. Instead of `trying to eradicate the unexpected, today's organizations need to anticipate and to prepare for unexpected challenges and opportunities — in other words, they need to be poised to adapt in a world where surprising challenges and innovative opportunities are normal.

We suspect that being resilient and ensuring compliance are two forces in conflict in today's world. So, how do we balance these pressures, when the pace of change accelerates, the scale of activities jump, and the complexity of interdependencies overwhelms analysis?

The program for the 7th SYMPOSIUM OF THE RESILIENCE ENGINEERING ASSOCIATION (REA) engaged participants in an energetic exploration of what it means to be poised to adapt in a turbulent world and how to resolve the conflict between adapting to be resilient versus the pressures for compliance with standards. In this document, we are pleased to proposed papers associated with some of the presentations made during the 7th REA symposium, but also all the abstracts of the conference's presentations and posters.

***Jean Pariès**, President of the Resilience Engineering Association and **Anne-Sophie Nyssen**, Host of the symposium*

Committees of the symposium

Programming and Scientific Committee

The Programming and Scientific Committee was responsible for designing and managing the program.

The members were:

- David Woods (chairman)
- Anne-Sophie Nyssen
- Matthieu Branlat
- Richard Cook
- Pedro Ferreira
- Ivonne Herrera
- Patricia Hirl Longstaff
- Chris Nemeth
- Jean Paries
- Gesa Praetorius
- Eric Rigaud
- Jan Maarten Schraagen
- Robert Wears

Organizing Committee

The Organizing Committee was responsible for the symposium project management, facilities, symposium website, sponsoring and communications.

The members were:

- Anne-Sophie Nyssen (chairman)
- Johan van der Vorm
- Arthur Dijkstra
- Mathieu Jaspar
- Pedro Ferreira
- Gesa Praetorius
- Eric Rigaud
- John van Schie
- Chrisine Goffinet

Young Talents Program Committee

The Young Talents Program aimed at organizing a workshop for young talents, MSc and PhD students working in the area of Resilience Engineering.

The members were:

- Gesa Praetorius (coordinator)
- Sudeep Hedge
- Matthieu Branlat
- Dianka Zuiderwijk

Keynote Speakers

David L. Alderson is an Associate Professor in the Operations Research Department and serves as Director for the Center for Infrastructure Defense at the Naval Postgraduate School (NPS). Dr. Alderson's research focuses on the function and operation of critical infrastructures, with particular emphasis on how to invest limited resources to ensure efficient and resilient performance in the face of accidents, failures, natural disasters, or deliberate attacks. His research explores tradeoffs between efficiency, complexity, and fragility in a wide variety of public and private cyber-physical systems. Dr. Alderson has been the Principal Investigator of sponsored research projects for the U.S. Navy, Army, Air Force, Marine Corps, and Coast Guard. Dr. Alderson received his doctorate from Stanford University and his undergraduate degree from Princeton University.

René Amalberti, born in 1952, is MD, PhD cognitive psychology, Professor of Medicine, physiology and aerospace medicine. After a residency in Psychiatry, he integrated the Airforce in 1977 and got a permanent Military Research position in 1982. He retired in late 2007. From 2008 to 2017, he was subsequently working as Senior Adviser Patient Safety at the Haute Autorité de Santé (HAS, French accreditation agency), and medical risk director in a Private Insurance Cie (MACSF). He is now fully retired, remaining Volunteer Director at the Public foundation for a safety culture in Industry (FONCSI) in Toulouse. He pioneered in the mid 80's the concepts of human error, ecological safety, crew resource management, and system safety. In late 1992, he was detached from the military to the European Joint Aviation Authorities (JAA) and became the first Chief Human factors and Flight safety of the JAA, then occupied a series of managerial positions in European and French research programs and administration (Land transport, Industrial and Environmental risks). In the late 90's, he moved his research to patient safety, system approach and resilience. He has published over 150 international papers, chapters, and authored or co-authored 10 books (last books: Navigating safety, Springer, 2013, Safer healthcare, strategies for the real world, Springer 2016).

Sidney Dekker (PhD The Ohio State University, USA, 1996) is professor of social science at Griffith University in Brisbane, Australia, where he runs the Safety Science Innovation Lab. After becoming full professor, he learned to fly the Boeing 737, and worked part-time as an airline pilot out of Copenhagen. He is best-selling author of, most recently: The End of Heaven: Disaster and Suffering in a Scientific Age (2017); Just Culture: Restoring Trust and Accountability in Your Organization (2016); Safety Differently (2015); The Field Guide to Understanding 'Human Error' (2014); Second Victim (2013); Drift into Failure (2011); Patient Safety (2011).

Gudela Grote is Professor of Work and Organizational Psychology at the Department of Management, Technology, and Economics at the ETH Zürich, Switzerland. She received her PhD in Industrial/Organizational Psychology from the Georgia Institute of Technology, Atlanta, USA. A special interest in her research are the increasing flexibility and virtuality of work and their consequences for the individual and organizational management of uncertainty. Prof. Grote is associate editor of the journal Safety Science and president of the European Association of Work and Organizational Psychology.

Erik Hollnagel is Professor at the Institute of Regional Health Research, University of Southern Denmark (DK) and Chief Consultant at the Centre for Quality, Region of Southern Denmark. Erik has for many years worked at universities, research centres, and industries in several countries and with problems from many domains including nuclear power generation, aerospace and aviation, software engineering, land-based traffic, and healthcare. He has published widely and is the author/editor of 24 books, including five books on resilience engineering, as well as a large number of papers and book chapters.

Jean Paries is the President of the DEDALE company, located in Paris (France) and Melbourne (Australia), and active in domains such as aviation, nuclear power, or patient safety. He is an internationally recognized expert in the field of Human and Organizational Factors of safety. He graduated from ENAC, the French National School of Civil Aviation, as an aeronautical engineer. Before leading Dédale, he worked with the French Civil Aviation Authority, then with the French Air Accident Investigation Bureau. Since the early 2000s, he has actively participated in the research movement of resilience engineering, and he is the current President of the "Resilience Engineering Association".

David Woods began developing Resilience Engineering as an approach to safety in complex systems in 2000-2003 as part of the response to several NASA accidents and is Past-President of the Resilience Engineering Association. He is Professor at the Ohio State University in Dept. of Integrated Systems Engineering.

Special Events

The Young Talent Program

A one day workshop for Master and PhD students during which students have been the opportunity to present their work to prominent researchers within the field of Resilience Engineering.

Capacity for resilience in jazz improvisation

The symposium ended with the musical intervention of **Steve Houben,** a music professor and worldwide famous jazzman, and **Quentin Liégeois**.

But also some particularly entertaining events….

The Curtius' Brewery Visit & Tasting

The Welcome Reception

The Gala Dinner

Brief Video Captures

Sponsors

Contents

Papers

CAN ARTEFACTS BE ANALYZED AS AN AGENT BY ITSELF – YES OR NO: WHAT DOES HUTCHINS 'HOW DOES A COCKPIT REMEMBER ITS SPEEDS' TELL US

Adriaensen, A. [1], Patriarca, R. [2], Smoker, A. [3], and Bergstrom, J. [4]

[1] Lunds Universitet, Division of Risk Management and Societal Safety, Sweden

adriaensen@me.com

[2] Sapienza University of Rome, Department of Mechanical and Aerospace Engineering, Italy

riccardo.patriarca@uniroma1.it

[3] Lunds Universitet, Division of Risk Management and Societal Safety, Sweden

anthony_john.smoker@risk.lth.lu.se

[4] Lunds Universitet, Division of Risk Management and Societal Safety, Sweden

johan.bergstrom@risk.lth.se

Abstract

This paper re-iterates Hutchins' study 'How a Cockpit Remembers Its Speeds' from 1995. This latter emphasized the unit of analysis in exploring the processes and knowledge structures that underpin the activity of a socio-technical system. Hutchins investigated this concept through conceiving the cockpit as a joint cognitive system: how this work-system observed and remembered the speeds by which the aircraft operated, with a focus on turning non-observable properties of system performance into adaptive strategies.

Hutchins' main conclusion was that "the classical cognitive science approach can be applied with little modification to a unit of analysis that is larger than an individual person" (Hutchins, 1995, p. 2). Starting from this macro-level conception about the joint system, our own study re-establishes that the unit of analysis in FRAM is functional, starting bottom-up by building a model of functions and inter-dependencies among agents, even at different levels of abstraction.

The novelty of this study is that the traditional boundary between medium and agent was abandoned in favor of accepting aircraft systems and artefacts as agents of their own, all entitled to produce functions in the FRAM model and how this effected task and information propagation.

1. INTRODUCTION: FRAM IN A NUTSHELL

FRAM and resilience engineering share several principles, from which the FRAM handbook lists the principle of equivalence, approximate adjustments and emergence. The abbreviation FRAM stands for Functional Resonance Analysis Method and carries two key concepts, functional-based approach and resonance. Resonance is used as an alternative to cause-effect relation and can be used to describe and explain non-linear interactions and emergent rather than resultant outcomes (Hollnagel, 2012). The other term 'function' deserves some further explanation. In FRAM, a function is presented by a hexagon and represents the acts or activities – simple or complex – that are needed to produce a certain result (Hollnagel, 2012). This can describe what people, organizations, technical or socio-technical systems do. Each hexagon form has six aspects: Input, Output, Requirements, Resources, Control, and Time. These are connected to each other by relationships. Some aspects can have more than one relationship, but not every single aspect (besides outputs) needs to be connected. The resulting dependencies are subjected to a non-linear analysis, in which it is important to note that the general principle is to analyze the task as it is carried out under normal conditions. FRAM's point of departure is not to describe incidents, but the work domain. However, anomalies can be analyzed as special instantiations of the model in comparison to the task as normally done. The power of the model lies in the fact that the whole model only consists of hexagons and the way their aspects are interrelated. FRAM is a method-sine-model rather than a model-cum-method (Hollnagel, 2012), thus allowing to study the full potential of resilience engineering, as there is no discrimination between positive and negative outcomes and hierarchical control dependencies are avoided. Every FRAM model is defined by boundaries that are chosen with the scope of the study in mind, but still need to be selected in such a way that the model contains enough functions to explain the task, yet not more than needed. The model does not allow lost functions with no connections, forcing the researcher to identify logic relations and still reach a 'closed' model at some point. In the original Hutchins' study, observational qualities were strong, but a rigid method was missing. The research question of our study is whether the

Hutchins' case can be described more methodically with the help of FRAM vocabulary and modelling. And concerning the FRAM methodology, can artefacts be analyzed as agents of their own? The remainder of the paper is organized as follows. Section 2 details the research method we developed starting from FRAM. Section 3 summarizes the results of the study, applied to the DC-9 cockpit, exploring the work-as-imagined and the work-as-done for speed setting. Section 3 also shows some potential guiding principles for the analysis, i.e. mechanisms. Lastly, the conclusions summarize the outcomes of the study and the potential for further research.

2. RESEARCH METHOD

Our research approach started from the concepts of information flow, transformation of information and distributed access to information in cockpits, as discussed in Hutchins' paper 'How a cockpit remembers its speeds' and Palmer's 'Altitude Deviations: Breakdowns of an Error Tolerant System', co-authored by Hutchins (Hutchins, 1995; Palmer, Hutchins, Ritter, & vanCleemput, 1991). Typical elements of information flows are clearances, instruction read-backs, instrument bug settings, analogic and digital instrument inputs, pilot checks, written checklist information, etc.

We firstly developed an ecologically valid FRAM model, based on work-as-imagined, by consulting company manuals and the expertise of one the researchers who also was an airline pilot, although not on the DC-9 aircraft. Thereafter, the model has been finalized describing work-as-done, thanks to the knowledge of three Subject Matter Experts (SMEs), i.e. former DC-9 pilots, involved in a focus group. The pilots, after a session discussing the theoretical background of FRAM, were interviewed to gain operational knowledge of the work domain. They were free to alter - even delete or add - any function and/or their aspects. Whereas the original Hutchins' paper was based on the MD-80 aircraft, we based our exercise on its predecessor, the DC-9 because it enabled us to work with three former DC-9 pilots from the same airline. This was needed to build an accurate work-as-done model dictated by a single set of company procedures and practices. When building the model, we supported our SMEs with cockpit training posters, cockpit pictures and copies of the actual company manuals.

Generally, FRAM researchers use FRAM Model Visualizer (FMV) to develop a model. However, for complex models characterized by many functions, FMV presents limitations on user-experience. Additionally, FMV is primarily aimed to analyze iterations (walk-throughs) of the model and to generate static relationship overviews, which can become visually overwhelming depending on the amount of functions and aspect. For the purpose of this study, one of the authors developed a VBA code, which interacting with FMV, was able to create a FRAM model, starting from a user-friendly data entry form in Microsoft Excel. Operationally, this means that all functions have been assigned to different levels of resolution (i.e. abstraction), through Excel fields tied to the functions. This complexity-management strategy was based on Rasmussen's Abstraction/Decomposition framework (Rasmussen, 1985), recently adapted in an Abstraction/Agency framework developed to give sense to the functional resonance space (Patriarca, Bergström, & Di Gravio, 2017). Since the abstraction level reflects the "lens" used to describe the work domain, we defined the abstraction layers after gathering data from the focus group. Possible ambiguities were discussed with our pilot informants, by semi-structured interviews.

The novelty of this study is that the traditional boundary between medium and agent was abandoned in favor of accepting aircraft systems and artefacts as agents of their own, all entitled to produce functions in the FRAM model. This allowed to analyze how task-relevant information moves "through the cockpit system by translating the representation of information in one medium to a representation in another" (Palmer et al., 1991, p. 18). Whether this information is than transformed through the process of human cognition, an aircraft system, or even an artefact makes no difference in terms of the model we developed. Although the FRAM handbook itself brings to the attention that functions can also describe technical systems (Hollnagel, Hounsgaard, & Colligan, 2014, p. 23), this paper radicalizes this possibility by defining artefacts and even environmental influences as agents of their own.

3. RESULTS

3.1. Speed setting-as-imagined

The work-as-imagined model in the company manual contains procedures, compact and expanded checklists, calculation tables and diagrams and detailed responses to a wide variety of circumstances. It is interesting that there is no part or a sum of parts of the company manual that fully explains to the pilots, the actual sequence of activities, schedules and events meant for speed control from the aircraft's Top of Descent (TOD) until landing. Even when this information is compiled from different parts of the manual, sometimes located far apart and in mixed forms of text and charts, the dynamic sequence of events involved could not be derived in all its aspects from the written procedures. In the company manual, one example being that there was no reference about

how exactly the approach descent checklist is triggered; even if this describes an essential part in the procedure. The lack of a full description demonstrates that aircraft handling is supplemented by a set of commonly shared procedures that are verbally communicated in on-the-job-learning and training, from which follows that a work-as-done model is a more accurate basis for this non-trivial task analysis.
The analysis of the company procedures and manuals reveals a sequential process paradigm. This can typically be found in speed reduction schedules from standard approach charts that depict the aircraft in relation to descent profiles or beacons. Another example is the chronological description of standard procedures per flight phase, accompanied by checklists. A further observation is that adaption to a wide variety of both standard and non-standard scenarios, is presented as fragmented information in the form of add-on descriptions or variations to a leading scenario. This decomposition of information contrasts with the dynamic sequence - not always sequential - of actions and events, by the work-as-done model contained in this study. Therefore, the information contained in the manual from both simple and complex procedures requires a cognitive translation into the actual dynamic processes they represent. Even if this company manual is already a few decades old and does not represent today's industry best practices, the decomposition of information remains undoubtedly a major challenge for all training purposes and company manuals. Not to mention that "[t]he work situation in large-scale socio-technical systems is partly intractable", meaning "that the conditions of work are underspecified, in principle as well as in practice" (Hollnagel, 2012).

3.2. Speed setting-as-done

Different datasets can be described, from which Hutchins used the particular example of the task propagation and information flow related to the memorization and utilization of speeds for the aircraft's approach and landing. Four years earlier he illustrated the same principle together with Palmer about altitude, instead of speed specifications:

> "Notice that the altitude specification is in some sense the "same" information whether it is represented in spoken words, as a string of written characters, or in the digits visible in the display window of the altitude alerter. A medium is said to represent some particular piece of information by virtue of having a particular physical state. For example, the altitude-alerter display window represents the altitude thirty-three thousand feet when the digits "33000" appear in order in the window. The crew moves information through the cockpit system by translating the representation of information in one medium to a representation in another" (p.18).

The description above is an insightful illustration how the same information becomes translated in different forms and can subsequently be used as the origin for possible paths that task-relevant information can take in the cockpit system (Palmer et al., 1991, p. 18) Hollnagel and Woods (2006) recognized the Hutchins study as one of three hallmark papers on cognitive task syntheses that later gave rise to frame JCS. Although Hollnagel et al. applaud the incredible quality of observation of those pre-JCS studies, they also note that in each of them any discussion of methods is virtually absent (Hollnagel & Woods, 2006, p. 39). In our current study this problem is resolved, by systemically analyzing each transformation of task-relevant information or a task-related-action with the help of FRAM functions. A complete walkthrough of the information, supported by figures and the full data would be too lengthy for the format constraints of this paper. One can also recognize in Figure 1 that the visualized model is beyond interpretation. Note that even then, the static visualization does not yet tell the full examination narrative. It is a supportive tool that initiates or accompanies the analysis. Therefore, Figure 1 is only provided at a small size-fitting scale to give the reader an understanding of the complexity of all relationships that were required in this specific task. In this data section, we will rather unravel some of the applied mechanisms and apply them to some examples.

3.3. Mechanisms for modelling and analysis

One of the challenges we encountered by studying other literature that made use of FRAM and in making our own FRAM model, is the fact that the method still leaves a certain degree of liberty in defining functions. This might affect the results in terms of reproducibility. We found that: i) the degree of granularity as processed in a function is underspecified, and ii) the choice for agents ranging from human to technical, although well-described by Hollnagel (2012), is rarely applied in other FRAM studies. With the mechanisms described below, we describe some guiding principles for the breakdown of steps when defining one or more FRAM functions, and we advocate radical freedom for the choice of agents that can drive functions.

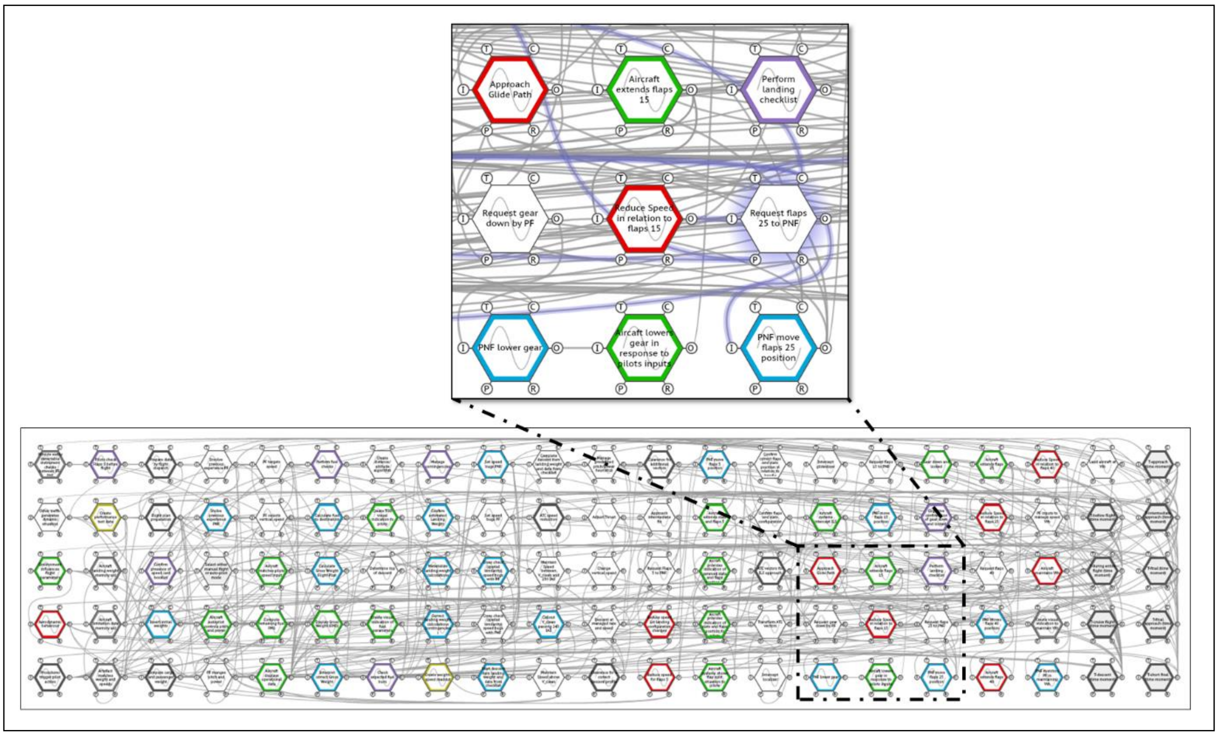


__Figure 1.__ The FRAM model for speed-setting in a DC-9 cockpit. Note how the graphical representation becomes overwhelming due to the huge number of functions and tight interactions among them. Note that each colour represents a different agent, according to a JCS perspective.

Mechanism #1: a breakdown of functions (the different steps in the task analysis) in its smallest significant parts.

For example, one could typically define in FRAM that the function <Set Flaps 25>, requires Input <Flaps position smaller than 25> and produces Output <Flaps 25 position>. However, it can also be described by describing several smaller functions. In our model, the initial general function has been broken down into the following steps, beginning with a function called <Request Flaps 25 to PNF>, requiring Input: <Reducing speed from Vp15 to Vp25 and below> and producing Output <Call out "Flaps 25">, by agent Pilot Flying (PF), i.e. PF slows down the aircraft and immediately requests the new flap setting to his Pilot Non Flying (PNF), followed by Function <PNF moves handle to flaps 25>, requiring Input <Call out "Flaps 25"> and producing Output <Flaps 25 handle position> and <Call out "Flaps 25 selected">, by agent Pilot Non Flying (PNF). Thereafter the agent <aircraft systems>, reacts with the function <Aircraft extends flaps 25>, requiring Input <Flaps 25 handle position> and producing Output <Flaps 25 extended left side> and <Flaps 25 extended right side>. This sequence of three functions equals one single function at the beginning of our example. Note that in our model the task has suddenly travelled through 3 agents, Pilot Flying, Pilot Non-flying and Aircraft systems, instead of one.

Mechanism #2: look for the function that requires the least processing effort (cognitive or computational).

So far, we have described that the aircraft has extended its flaps at the left and the right side. However, we have not described in which way the pilots receive feedback from the aircraft systems to tell them that the flaps, which to them are out of sight, actually are in the desired position. Therefore, the pilots need to check that the flaps indicator (e.g. Flaps 15 instrument indication pointer) corresponds to the correct handle position (e.g. Flaps 15 dent position). Although this single confirmation appears sufficient, chances are high that a physically blocked flap also causes an asymmetry. In this case, the pilots would immediately see that the two pointers on the flap indication instrument would not be aligned. Verifying the spatial similarity of two overlapping pointers on a single dial is translated in the verification that <Flap pointers left-right show no split>, a typical example of something that hardly requires any cognitive computation. ‘Pattern matching’ of two aligned pointers is cognitively less demanding and less prone to error, compared to checking a flap handle position (at a head-down visual position), with 2 pointers on the flap indication instrument (at a heads-up visual position). But at the same time checking the handle position is more thorough, because it includes the scenario where 2 flaps would have failed symmetrically. Note that it is therefore not strictly necessary to create the <Flap pointers left-right show no split> function, because it is superfluous to the confirmation of checking the flap pointer indications with the respective handle position and it would not appear in a work-as-conceived model. However, this two-step efficiency-thorough checking is how cognition really functions in this case, according our SMEs, and therefore we must add one step to the work-as-done model. FRAM does not tell us to add this step, and chances are likely that our SMEs would even overlook this step if not confronted with the right interview questions. One could say that it was Hutchins that unveiled how cognition is often not the "reconstruction of some internal representation", but rather a "combination of recognition, recall, pattern matching, cross modality consistency checking" (1995, p.18). Therefore, Hutchins in return learned us how to better define FRAM functions that involve cognitive processes.

Mechanism #3: the principle of agent-neutrality.

Now we go back one step back in the model to the end of example #1. The function <Aircraft provides indication of flap position to pilots>, receives Inputs were already produced at the end of #1 with <Flaps 25 extended left side> and <Flaps 25 extended right side>, as outputs of the preceding function. This function in turn produces the Outputs <Pointer indication of slats and flaps left side> and <Pointer indication of slats and flaps right side>. This is followed by the Function <Aircraft systems shows flap split situation to pilots>, with the Input <Pointer indication of slats and flaps left side> and <Pointer indication of slats and flaps right side> and the output <Flap pointers left-right show no split> or in case of a contingency <Flap pointers left-right show split>. Only thereafter it becomes one out of several Controls that the pilots (PF) receive as the Function <Confirm the flaps and slats configuration>. Note that by abandoning the traditional boundary between medium and agent, there is little cognitive difference in labelling the aircraft systems' function which <*shows* flap split situation to pilots> on the one hand, and the function of the human pilot agent who <*confirms* the flaps and slats configuration>, by means of the Control, i.e. <Left-and right-hand side pointers are aligned>. This is not to say that there is no minimal cognitive processing involved in pointer checking, but the model treats human and technical processes equally.

Mechanism #4: consider parallel sequences of functions for (apparently) symmetrical tasks.

We often created parallel sequences of tasks for PF and PNF, even if both pilots performed identical tasks. When a checklist says that speed bug settings need to be cross-checked, one could define a single function for that cross check, but due to the trajectory of information and/or tasks, we found that such symmetries were often discontinued a few functions away, downstream or upstream. In our model, PF and PNF for example, received separate cross-check functions for this reason. <Cross check speed bug settings between PF – PNF> is an equal but distinct activity for both pilots. However, downstream the PNF starts using these bugs as a retained memory aid for monitoring his PF, which then ceases to be a reciprocal function. Upstream such crosschecks are linked to checklist actions which are not symmetrical. This happens by the very nature of challenge and response type checklists. However, even in this study, some functions handled by both pilots were still allocated to a single function, and as a consequence, a single agent <joint pilot team>. The motivation could be that they happened at an abstraction level from which no physical functions were defined. This is for example true for contingency management, which this model did not further investigate beyond defining such contingencies.

3.4 Propagation of tasks

Central in this study are the speeds used for controlling and landing the aircraft and how they are memorized. "In order to maintain safe flight at slower speeds, the crew must extend the slats and flaps to produce the appropriate wing configurations at the right speeds" (Hutchins, 1995, p. 4). The appropriate speeds differ with varying aircraft's weight and will be calculated just before or after the descent point. In the MD-80 example from the Hutchins study, the transformation from the landing weight into the accompanying speeds is accomplished by a very effective artefact, a booklet of speed cards. "The booklet contains a page for each weight interval (usually in 2,000 pound increments) with the appropriate speeds permanently printed on the card" (1995, p.5). The DC-9 example used in our study, had a nearly identical booklet. Turning the booklet on the correct page simply means that the pilots have the correct landing speeds displayed. The booklet is then positioned on a prominent place in the cockpit. The speeds from the booklet serve to set the speed bugs, another simple, but effective memory aid. The speed bugs, are moved by a rotating knob and physically positioned around the analogue Air Speed Indicator (ASI) dial. Both pilots have their own ASI, each with their own set of speed bugs.

In Hutchins view, this makes the system redundant in memory and processing and provides more redundant checks. "The interaction of the representations in the different media gives the overall system the properties it has" (1995, p. 19). The propagation of tasks can be seen as a set of transformations of information flows and the pilots' reactions to these changes. Speed bugs become involved in a distribution of cognitive labor across social space and "the cognitive work of reading the airspeed indicator, and monitoring the other instruments on the final approach can be divided among the pilots" (1995, p. 19). Speed bugs do not help pilots remember speeds, rather they are part of the process by which the cockpit system remembers speeds. Also, "speed bugs permit a shift in the distribution of cognitive effort across time. They enable the crew to calculate correspondences between speeds and configurations during a low workload phase of flight, and save the results of that computation for later use" (1995, p. 19).

A central question is if a FRAM model can handle a similar propagation of tasks. The answer is that a FRAM model can certainly be read as a propagation of tasks, although the relations must not necessarily be read as sequential steps. The FRAM model allows to depict non-linearity when the output of functions leads to several Preconditions or Controls for impending functions. For example, in the case of a Precondition, this does not necessarily define a tight sequence, but it creates a condition for certain functions that cannot be started before other critical functions are fulfilled.

Furthermore, when Hutchins' less systematic, but more descriptive approach would be translated into FRAM, his transformations of information would be mere Inputs and Outputs, whereas (e.g.) one could describe the crosschecks between pilots as Controls. FRAM vocabulary has several other aspects and thereby has a richer potential for describing dependencies and exploring the work domain. Even a pilot crosscheck, intuitively thought as a Control, might be a Precondition for another function and thereby have the control to start or delay a specific task. This gives FRAM, in contrast to the Hutchins, the opportunity to describe non-linear relations.

4. CONCLUSION

Hutchins described 3 accounts to "examine the activities in the cockpit that are involved with the generation and maintenance of representations of the maneuvering and reference speeds" (1995, p. 5): 1) a procedural description of memory for speeds; 2) a cognitive description by means of representations and processes outside the pilots and; 3) the same by representations and processes inside the pilots. He dismissed all three in favor of a system-level cognitive view that "directs our attention beyond the cognitive properties of individuals to the properties of external representations and to the interactions between internal and external representations" (Hutchins, 1995, p. 20). This study not only agrees with this, but included these findings in its methodology. We dismissed a procedural description by starting from a work-as-done model and we were mindful not to use FRAM functions that would represent possible opaque cognitive processes. In fact, FRAM allowed us to treat the transformation of energy or information by human agents, aircraft systems or artefacts as agent-neutral transformations and thereby avoided the use of cognition in its classic sense. By using FRAM as a model or even a language to treat humans and machines as equivalent producers of functions, the joint performance of the system can be described as the net result of the resonances between functions. FRAM proved to be a tool that allowed to study JCS more systematically. However, this implies that some pre-concepts, which we described as a set of mechanisms to define FRAM functions are aligned with JCS. At this point, FRAM itself does not tell us something about those choices and this study benefited from studying the JCS concepts. The results of this study should offer future researchers a chance to determine a level of granularity about the unit of analysis, in relation to the question which agents are entitled to create functions. The model developed in this study, might be helpful to gain in-depth knowledge of the work domain, with potential implications for both organizational learning and safety management, using the cited mechanisms.

REFERENCES

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*: Ashgate Publishing, Limited.

Hollnagel, E., Hounsgaard, J., & Colligan, L. (2014). *FRAM – the Functional Resonance Analysis Method – a handbook for the practical use of the method*: Centre for Quality, Region of Southern Denmark.

Hollnagel, E., & Woods, D. D. (2006). *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*. Boca Raton; London; New York: Taylor & Francis.

Hutchins, E. (1995). How a cockpit remembers its speeds. *Cognitive Science, 19*(3), 265-288.

Palmer, E. A., Hutchins, E. L., Ritter, R. D., & vanCleemput, I. (1991). Altitude Deviations: Breakdowns of an Error Tolerant System: National Aeronautics Space Administration and U.S. Department of Transportation Federal Aviation Administration.

Patriarca, R., Bergström, J., & Di Gravio, G. (2017). Defining the functional resonance analysis space: Combining Abstraction Hierarchy and FRAM. *Reliability Engineering & System Safety, 165*, 34-46.

Rasmussen, J. (1985). The Role of Hierarchical Knowledge Representation in Decisionmaking and System Management. *IEEE Transactions On Systems, Man, And Cybernetics, 15*(2), 234-243.

RECRUITMENT, SELECTION AND TRAINING OF NEW WORKERS BASED ON RESILIENCE SKILLS: A STUDY WITH GRID ELECTRICIANS

Alexandre E. Alves[1], Tarcisio A. Saurin[2], Marcelo F. Costella[3]

[1, 2] Federal University of Rio Grande do Sul, Av. Osvaldo Aranha, 99, 5. andar, CEP 90035-190, Porto Alegre, Brazil

[3] Universidade Comunitária da Região de Chapecó e Faculdade Meridional IMED, Av. Atilio Fontana, 591-E, Chapecó, Brazil

[1]alexandre.eberle@terra.com.br, [2] saurin@ufrgs.br, [3] costella@unochapeco.edu.br

Abstract

In this paper, we discuss the role played by the recruitment, selection, and training (RST) in the use of resilience skills (RS) by electricians and control room operators who perform emergency maintenance activities in an electricity distribution company. This investigation was based on a field study which involved three main steps: (i) characterization of the requirements the company posed for the RST of new workers; (ii) identification of RS demanded by electricians and control room operators, as well as the work constraints these face in every day work; and (iii) crosschecking of the data in step (i) with the data of step (ii), which allowed evaluating if and how RS and work constraints were accounted in the RST of new workers. This comparison indicated that all RS were partially covered by the psychological tests, even though these had greater emphasis on personality traits, reasoning and memory. Furthermore, a training program which accounted for the last stage of the selection of new workers was changed in order to explicitly include work constraints and request the use of the RS identified in the data collection. As a result of this change, 10% of the 215 applicants studied were considered as inapt during this late stage of the RST process. This is in contrast with the 1% fail rate that was previously common in the company.

1. INTRODUCTION

Resilience skills (RS) are defined as skills of any type necessary to adjust performance, in order to maintain safe and efficient operations during both expected and unexpected situations [Saurin et al., 2014]. From the resilience engineering (RE) perspective, the unit of analysis for studying RS should be the joint cognitive system (JCS) formed by the interactions between the individual professional and his social and material environment. Therefore, data collection for the identification of RS should be concerned not only with the RS themselves, but also with the context in which they are deployed [Wachs et al., 2016].

In this work, the RS subject is studied in an electrical power distributor. The complexity of the work involved in power distribution is worth noting, with maintenance being carried out because of equipment failure and with a constant demand for speed in the restoration of the system to service the company's customers. This generates operations under high pressure for completion of the work in the shortest time possible, with risks of serious accidents and damage to equipment and personnel during its execution, and, above all, in an environment with constantly changing conditions.

Additionally, the energy distribution activity has a quite peculiar characteristic, since the priorities are dynamic during the execution of the work. For example, at a given moment the focus of the work may be the restoration of electricity to a school, but if the blackout on a hospital occurs, this priority will be changed and most efforts will be quickly redirected. Furthermore, companies of the electrical sector are subject to the application of penalties by the federal government, and the system is often operating close to its physical limits, with its operation being increasingly subject to such phenomena as: the loss of synchronism, drops in frequency, tension collapse, cuts of generators and charges. The operation of an electrical power distributor is also strongly affected by climatic conditions, which can cause a large volume of problems to occur simultaneously. There are also cases where a delay in action by the distributor can cause fatalities. These kinds of cases occur, for example, in situations where powered lines are on the ground due to a broken wire, accessible to people in the community. This may result in accidents, especially to those who lack the knowledge and awareness regarding the dangers of electricity.

Because of these characteristics and also due to the adversities encountered during the activities of the electricians in the field and the control room operators (CRO), this is a field a knowledge that is quite aligned with the study of resilience skills. Technical training alone is not able to cover all situations encountered in the varied universe faced by the field teams.

The recruitment, selection and training (RST) of new workers is an important part of this context, for two reasons: (i) hiring workers who are unqualified for their jobs is likely to require unnecessary and reactive resilience from their coworkers; this may imply an additional workload, safety hazards and the excessive use of resources in order to get the job done; (ii) personal characteristics matter in the performance of high-risk JCS, even though they are not stressed by RE, which emphasizes the organizational context.

In this paper, we discuss the role played by RST in the use of RS by front-line workers who perform emergency maintenance activities in an electricity distribution company. Said workers involve electricians who work in the field (usually in pairs) and control room operators at the company´s headquarters. These workers must work in close collaboration and synchronization.

2. RESEARCH METHOD

The study was conducted in a public electric power distribution utility in Southern Brazil, which is active in 21 countries with approximately 25.000 employees. The power distributor under study operates in an area of 99,512 km2 and services nearly 1.270.332 customers distributed in 118 municipalities. The analysis occurred in an operation that has been going on for 18 years.

The field study involved three main steps: (i) characterization of the requirements the company imposed for recruiting, selecting, and training new workers; (ii) identification of the RS and work constraints demanded from electricians and control room operators; and (iii) crosschecking of the data in step (i) with the data of step (ii), which allowed evaluating if and how RS and work constraints were taken into account in the RST of new workers.

Sources of data involved: (a) about 50 hours of participant observations, which were carried out by the first author of this paper, who was the company´s training coordinator; (b) analysis of documents that described how the RST should be carried out; (c) twelve interviews using the Critical Decision Method (CDM)[Crandall et al., 2006] with five electricians, five control room operators, and two psychologists who worked at the company´s human resources department, which was directly involved in the RST of new workers; (d) data regarding the performance of workers who participated in the RST over a seven-month period, including 450 applicants for the electrician job and 80 applicants for the position of control room operator.

Interviews and notes from observation diaries were subjected to a content analysis, in which the RS and work constraints which triggered their use were identified based on the method proposed by Wachs et al. (2016). When the recordings and transcriptions of the generated audio files were concluded, they were all analyzed and the relevant excerpts of text were classified according to the resilience skills and work constraints.

Using this data, changes were proposed in the training process and in the filters applied during the qualification of the professionals being trained. This was facilitated by the fact the first author, as the manager responsible for the training of company's professionals, had the authority to change the studied process of RST of new workers.

3. RESULTS

3.1. Characterization of the Company Requirements for RST

It is important to understand the duties of electricians in the field and the control room operators (CRO), which should operate in sync, to assess the recruitment and selection process. The main activities of electricians consist in the mounting and installation of pylons and structures to support suspended lines and the operation of suspended networks of de-energized or energized low voltage distribution systems. On the other hand, the CRO technicians manage the dispatch of service orders, the emergency dispatch and the coordination and control of the handling of the equipment of the distribution network.

The selection process of new professionals is managed by the Human Resources (HR) department, and their technical and education requirements are tested during the process. With respect to the psychological tests, the following skills are required:

- for electricians: leadership, negotiation, communication, customer focus, initiative, capacity for analysis and planning, decision making and interpersonal relationship skills.

- for the CRO technicians: confidence, interpersonal relationship skills, operational discipline, capacity for analysis and planning, emotional balance and management of work under pressure.

As shown in the research method, a group of 450 candidates who intended to participate in the electricians training course was assessed, in addition to 80 candidates for the technical CRO position (results shown in Table 1 and Table 2).

Table 1 *Result of the Electrician Admission Tests*

Participants	Failed Psychological Test	Failed Physical Test	Failed Driving Test	Failed Medical Assessment	Failed due to bad professional references	Deemed suitable by the end of the process
450	106	40	20	82	74	215

As can be seen, among the 450 professionals interested in becoming electricians who presented resumes to the distributor, only 47% were deemed suitable for the activity. It should be noted that some candidates were disqualified in more than one test. The approved candidates were referred to the qualification training, where another filter was applied, which, on average, removed approximately 10% of the aspiring candidates per class.

Table 2 *Results of the CRO technician admission tests*

Participants	Curriculum Evaluation	Failed Interview	Failed Psychological Test	Failed Medical Assessment	Professional References	Interview with department manager
80	65	4	1	1	0	2

The difference in the failure rate in psychological tests between the two activities (23.53% and 1.25%, for electricians and CRO, respectively), in addition to the differences in profile and the nature of the tests, can be explained by the education level. A significant portion of the public that pursues an electrician course completed their studies when they were already adults. In the period that they should have developed in school, they were deprived this opportunity, which, according to the psychologist responsible for recruitment, directly impacts their performance in one of the psychological tests with the highest failure rate: logical reasoning. The control room operators, on the other hand, were not only younger candidates, but they also had the prerequisite of a minimum level of technical education.

3.2. Identification of RS

The resilience skills of the electricians and CRO technicians are presented in Figure 1. The identified categories of RS are similar to those obtained by Wachs et al. [2016]. Figure 2 describes the work constraints cited by the respondents. The work constraints should be handled by the Company, whether through training or managerial actions, depending on the case, in order to avoid employees from having to use resilience skills to overcome them.

1 - Assuming leadership.
2 - Managing to keep attention focused on the task.
3 - Establishing priority actions.
4 - Identifying failures in procedure, in communication, in the system, in equipment, in the limits of the body/mind, and/or in other factors that hinder the work, in addition to respecting the procedure manual.
5 - Having a working method, doing planning, connecting information to search for the best way to accomplish a task.
6 - Managing conflict, helping/assisting colleagues, working on professional relationships, having the maturity to give and receive feedback.
7 - Dealing with teams or managers without the proper training or skills for the activity, in addition to anticipating the possibility of failure.
8 - Dealing with incidents, accidents and/or deaths with colleagues or people in the community.
9 - Keeping alert for the need to act in unexpected situations, including the lack of resources, in addition to always watching/checking if the procedures/tools are adequate.

10 - Having a perception of the activity's risks, in particular in moments of high demand, with a non-standard or run-down grid, in flooded, dark and/or hard to visualize places.
11 - Coping with pressure.

Figure 1. *Resilience skills*

Work Constraints
1 - Colleague who doesn't help, doesn't have the proper training for the job or has trouble with interpersonal relationships.
2- High work volume.
3 - Failures in the system and/or in communication.
4 - Work at night, in the rain, with the presence of animals or in flooded terrain.
5 - Use of new technology without grounding points.
6 - Working with old, run-down and/or non-standard networks.
7 - Working in places with difficult access.
8 - Working while having to request support regarding interpersonal relationship and not for processes and responsibilities.
9 - Working without all the required resources.
10 - Working under pressure and/or for several consecutive days with a high degree of stress.

Figure 2. *Work constraints*

3.3. Crosschecking of the data

The requirements in the psychological tests were crosschecked with the resilience skills identified (Figure 3), both for the electricians and for the control room operators. This comparison indicated that all 11 RS were at least partially covered by the psychological tests, even though these placed more emphasis on personality traits, reasoning and memory. It is worth noting that the lack of consideration of some RS in the RST process, could imply the emergence of some of the identified work constraints in the future. For instance, the RST evaluated how applicants performed in teamwork activities during the training course, while a lack of collaboration from coworkers was one of the work constraints identified in the data collection.

	RS1	RS2	RS3	RS4		RS5		RS6		RS7	RS8	RS9	RS10	RS11
Communication				Elect.										
Customer focus			Elect.											
Initiative						Elect.								
Leadership	Elect.													
Decision-making												Elect.		
Capacity for analysis and planning				Elect.	CRO	Elect.	CRO					CRO	CRO	
Interpersonal relations								Elect.	CRO					
Operational discipline		CRO												
Emotional balance										CRO	CRO			
Management of work under pressure														CRO
Safety												CRO	CRO	

Figure 3. *Crosschecking of the data: RS versus psychological tests requirements*

3.4. Changes in the training process

The training process of the electricians consists in a 362-hour training course, 192 of which theoretical and 170 practical. For the CRO technicians, the theoretical and practical training were 180 hours each, totaling 360. Both trainings have a high on-the-job portion.

One of the improvements proposed was the implementation of a training system that seeks to develop stress management skills for CRO technicians. This action seeks to improve the RS presented in item 4.1.2 regarding establishing priority actions (RS - 3) and coping with the pressure (RS - 11), since these skills can be trained and improved in a controlled environment with a simulator, before being experienced in a real-life situation.

Four suggestions were proposed for the training of electricians: inclusion of a nocturnal module, simulation of working-at-height activities before climbing the pylons, inclusion in the training center of simulations closer to those found in reality, and resilience skill assessments.

The inclusion of a nocturnal module is due to the fact that the maintenance activity from the distributor occurs 24 hours a day and electricians need to be prepared to work at any time and in all weather conditions. Therefore, the candidates would use the technical skills in another reality, where visibility is reduced and, as such, other difficulties are added, such as the need to use artificial lighting. It should be noted that rains and storms may eventually occur during the night module, as was the case experienced by one group of candidates followed by the researchers. The creation of this module, therefore, is one of the actions implemented by the distributor's training department in alignment with the resilience skill result, in particular in moments of high demand with a non-standard or run-down network in flooded, dark and/or with difficult to visualize places (RS - 10); as well as with the work constraint regarding the carrying out of night work, in the rain, with the presence of animals or in flooded terrains (Work Constraint- 4).

The simulation of activities at heights before climbing poles was proposed because of the fear of heights reported by some candidates for the electrician position. In order to assist in the development of this technical skill and facilitate activities at higher levels, the beginners are tested and monitored in a work simulation on the ground, but simulating other work conditions on the highest parts of the pylons. This way, electricians could get a feel of the safety equipment, gain confidence, and acquire the technical skills required to perform the task. In light of the above, this change in training is aligned with the resilience skill regarding the identification of the limits of the body/mind, and/or other factors that hinder the work (RS - 4), improves the training to avoid having to deal with a team without the proper training or skills for the activity (RS - 7) and also with a colleague who does not have the proper training for the job (Work Constraint - 1).

The redesign of the training center with simulations closer to those found in reality meets the demand that scenarios should reflect the challenges encountered in practice, in addition to the information received during the interviews that "when you are in a training, the network is completely clean there. Then, you arrive in the field, there are telephone lines, there is public lighting, there is a (cluster) of extensions on the pylon." For this reason, lighting fixtures were installed that are widely used in public lighting and cables that simulate telephony lines, hanging below the low-voltage grid, just as extensions were added to the pylons of the training center. This new configuration makes it difficult to carry out the tasks. As such, the practical activities offered at the Training Center were closer to the conditions experienced by electricians in their places of work. This action seeks to improve the RS regarding the identification of factors that complicate the work (RS - 4), just as the work constraint of working in places of difficult access (Work Constraint - 7).

The resilience skill assessments in the training had a direct impact on the fail rate of the electrician training course of the electrical power distributor under study. Prior to this new form of management, fail rates were rare (less than 1%). Currently, the fail rate is approximately 10% per class.

The coordinator of the department, along with the training analyst and instructors, has begun holding a class council at the end of each training class, discussing and checking the comments of each instructor who participated in the training of the students. The technical evaluation assesses whether the candidate electrician has acquired the necessary dexterity required to handle the equipment. However, the big difference deployed is the monitoring/evaluation of other items, such as: teamwork, initiative/engagement/interest, interpersonal relations, communication, discipline/compliance with standards and rules, attention and focus on the activity, agility and productivity, punctuality and attendance, attitude and personal presentation.

4. CONCLUSIONS

This work has discussed the evaluation method in the selection process of the electricity distributor under study, presenting the tests and requirements for the functions analyzed, in addition to further exploring the resilience skills necessary to carry out the activities of electricians and control room technicians.

A convergence was observed between the developed resilience skills and the variables observed in the psychological tests conducted by the company, contributing to a better selection of the candidates. In addition, changes occurred in the training process of the company where this study was carried out. Changes that sought to improve the resilience skills of the professionals trained by the Corporate Education department. As could be seen in the course of this study, other suggestions for changes in the development training were also generated, which are being analyzed and could potentially be implemented.

REFERENCES

Crandall, B., Klein, G. & Hoffman, R. R. (2006). *Working Minds: A Practitioner's Guide to Cognitive Task Analysis.* USA: MIT Press.

Saurin, T. A., Wachs, P., Righi, A. W. & Henriqson, É. (2014). The design of scenario-based training from the resilience engineering perspective: A study with grid electricians. *Accident Analysis and Prevention*, 68, 30-41.

Wachs, P., Saurin, T. A., Righi, A. & Wears, R. (2016). Resilience skills as emergent phenomena: A study of emergency departments in Brazil and the United States. *Applied Ergonomics*, 56, 227-237.

SUPPORTING RESILIENCE MANAGEMENT THROUGH USEFUL GUIDELINES

Matthieu Branlat [1], Rogier Woltjer[2], Luca Save[3], Odeya Cohen[4] and Ivonne Herrera[1]

[1] SINTEF, Strindvegen 4, 7034 Trondheim, Norway
matthieu.branlat@sintef.no, ivonne.herrera@sintef.no

[2] Swedish Defence Research Agency FOI, Stockholm, Sweden
rogier.woltjer@foi.se

[3] Deep Blue SRL, Piazza Buenos Aires, 20, 00198 Roma, Italy
luca.save@dblue.it

[4] Ben-Gurion University of the Negev, P.O.B. 653 Beer-Sheva, Israel
odeyac@bgu.ac.il

Abstract

The paper describes an on-going project, DARWIN, which is developing resilience management guidelines for the context of crisis management. The project started with a vast review of associated literature, standards and operational documentation, as well as interviews of practitioners. Numerous requirements were identified, in particular to capture resilience management capabilities the guidelines should address. The context is that of organisations that already have a number of processes and tools in place to support their management of crises (e.g., preparation activities, contingency plans, procedures, learning activities). As a result, the guidelines are positioned at a meta-level: they provide a perspective on these processes and tools grounded in research and practice on resilience management inspired by the fields of Resilience Engineering and Community Resilience. The paper describes the nature of the guidelines, established development and evaluation process, and components of the guidelines defined through an iterative discovery process. These different aspects aim at ensuring the usefulness, i.e. applicability and usability, of the DARWIN guidelines.

INTRODUCTION

The use of the term *resilience* has emerged during the last decades as a complementary concept for industry and society to improve beyond the limits of the prevalent approach to risk and crisis management, although the concept of resilience is however used widely differently in diverse areas of research and in response to different challenges (Woods, 2015). DARWIN, the on-going European project which is the topic of this paper, postulates that resilience has a reflective quality: resilient systems have the ability to manage their own resilience (Woods and Branlat, 2011). DARWIN aims to build resilience management guidelines to support critical infrastructure organizations in developing and enhancing their resilience in the context of crisis management. The project focuses on a proactive approach for dealing with disturbances and assumes that surprises are an inherent characteristic in these situations. Trends that have influenced calls to operationalize resilience include (Boin & McConnell, 2007; Herrera *et al.*, in press):

- the changing nature of societal risks to higher complexity, difficulty in predicting occurrence and impact, and increased interdependencies in occurrence, impact and response;
- the awareness of limitations in prevalent risk-based approaches that emphasize the predictability of risks' occurrence and impacts, but downplay rare events, systemic and emerging risks, and risk controversies;
- the insufficient ability and increasing demands to learn and evolve from experience from these types of crises and limitations of prevention and planning;
- the complexity and risk of propagation of everyday performance variability and cascading across boundaries to other systems (making prevention, mitigation, and preparation very challenging).

In the context of these trends in modern-day crises and accidents, the DARWIN project bases its development of Resilience Management Guidelines on two major strands of research: The Resilience Engineering perspective, and the body of knowledge on Community Resilience. Both traditions are particularly relevant to the context of crisis management due to their respective topics of interest, concepts and methods.

During the first 6 months of the project, a vast review of Resilience Engineering, disaster resilience, community resilience, and associated literature, standards and operational documentation, as well as interviews of practitioners, was undertaken (DARWIN, 2015). A significant number of requirements were identified, then selected via a modified Delphi process (see Adini *et al.* ,2017 for more details). The process resulted in an overall set of 51 items that were recommended for inclusion in resilience management guidelines in order to guide the subsequent development of the DARWIN guidelines (DARWIN, 2016). Those requirements included especially conceptual requirements that captured resilience management capabilities the guidelines should address, i.e. specific objectives for their content. Other requirements addressed, for instance, the form or quality of the guidelines, or their development and evaluation process. However, the requirements did not specify the nature of the guidelines, i.e. the object of design, in order for them to be useful. The development of such object is a typical "ill-defined" problem, i.e. corresponds to a problem for which there is no clear end goal, nor clear path to a solution. The nature of such problem is further complicated by the typical scope, scale and complexity of the domain of crisis management for which the guidelines are developed. As a consequence, the development process was an iterative discovery process, during which the team made attempts and learned about what the end-product (the guidelines) should be, as well as about the process to reach a satisfying solution.

The objective of this paper is to describe the approach adopted to ensure the guidelines are: (1) relevant to the objectives and effective at operationalizing resilience concepts, methods and tools (see section 2); (3) developed with operational needs in mind (see section 3); provided in a usable form and able to evolve (see section 4).

DEVELOPMENT OF RESILIENCE MANAGEMENT GUIDELINES

Object of design

The guidelines offer a critical overview of an organization's activities from the standpoint of resilience management, with the aim to effectively assist it in the creation, assessment or improvement of its own processes and documents. In other words, we are not developing guidelines for crisis management per se, but rather guidelines at a meta level: the context is that of organizations that already have a number of processes and tools in place to support their management of crises (e.g., preparation activities, contingency plans, procedures, learning activities). As such, the DARWIN guidelines can be complementary to existing guidelines or procedures in an organization, but they do not replace them. The guidelines are directed towards critical infrastructure managers, crisis and emergency response managers, service providers, first responders and policy makers. They provide these actors of crisis management with a perspective on these processes and with tools grounded in research and practice in resilience management.

To define such guidelines, the DARWIN project is developing Concept Cards (CCs), which propose interventions that can be implemented in order to reach the resilience management capabilities described by the requirements. While requirements define *what* needs to be addressed, the CCs describe *how* it can be done. Specific interventions are proposed for the different phases of the crisis (the pre-emergency period, the crisis itself, and the post-emergency period), as well as across phases when relevant.

The CCs constitute the building blocks of the guidelines, and describe their conceptual framework. The guidelines form a holistic perspective, and capture the relationships between the CCs. Indeed, conceptual requirements don't stand alone, because the resilience management capabilities they refer to are not independent. For instance, the management of adaptive capacity requires that coordination be properly supported between operational units; these types of resilience management capabilities are different, but interdependent (Woods and Branlat, 2011). Many similar relationships can be found between CCs. A central component of the guidelines is a conceptual map that organizes the CCs; it is used both for knowledge representation and development purposes. In addition, categories are used to qualify and organize the CCs: general themes, functions of crisis management, resilience abilities, and users. Those categories play a central role in the access to the information provided by the guidelines (e.g., navigation with the content).

The last component of the guidelines is a web platform that aims to facilitate the development and future use of the guidelines (see section 4 for details). The platform is an inherent part of the guidelines, because it changes their nature, content and associated capabilities, especially compared to more traditional document formats.

Guidelines development process

The guidelines development process has evolved significantly from the beginning of the project. We summarize here the current 4-step iterative process that organizes the two core tasks: the development of CCs and updating of the guidelines conceptual map (see DARWIN D2.1, 2017 for more details).

The *1st step* is the selection of an undeveloped capability described in a requirement. Efforts are initially made to collaboratively agree on the meaning and intent underlying the description. These efforts might lead to the decision to develop a CC, or to drop the requirement, e.g., based on the fact that the corresponding capability is covered by another CC. In the latter case, the guidelines map is updated and another resilience management capability is considered.

The 2^{nd} *step*, the development of a draft CC, is a collaborative and iterative process within the development team, which involves different DARWIN consortium members, presenting various perspectives on the resilience management approach. It consists essentially of finding relevant content in the material captured during the initial literature review and interviews, then synthesizing this content in the appropriate fields of a template. This content is complemented when appropriate based on the knowledge and experience of persons involved in the development (e.g., knowledge of a relevant resilience management practice identified in previous work). In addition to the interventions proposed, the CC include a wide range of information, including: purpose and rationale; sources of information used in the development; targeted actors of crisis management; associated functions of the crisis management; expected benefit; associated challenges.

The 3^{rd} *step* is the revision of a CC based on its presentation to operational experts once it has reached sufficient maturity. Three main types of events provide such opportunities: efforts to adapt the CC to the domains of healthcare (HC) and air traffic management (ATM), carried by end-user organizations in DARWIN; evaluations carried within the project (see next section); events with the DARWIN Community of Practitioners (DCoP), experts from various academic and operational domains. These are all opportunities to gather early feedback (vs. only for a more finalized product) and lead to new cycles of collaborative revisions of the guidelines' content.

Finally, the 4^{th} *step* is the revision of the guidelines map. The development of a CC generates new knowledge and understanding about the overall guidelines. It can for instance lead to the identification of relationships with other content, or of a resilience management capability not previously captured in the map.

Current guidelines' content

The DARWIN Resilience Management Guidelines, in their current form (DARWIN D2.1, 2017), provide guidance on the following themes and associated resilience management capabilities:

- *Supporting coordination and synchronisation of distributed operations*: Ensure that the actors involved in resilience management have a clear understanding of their responsibilities and the responsibilities of other involved actors; promoting common ground in cross-organizational collaboration in crisis management; and establish networks for promoting inter-organizational collaboration.
- *Managing adaptive capacity*: Adapt to both expected and unexpected events (all-hazard approach), and adapt relative to procedures.
- *Assessing resilience*: Identifying sources and manifestations of brittleness and resilience, for organisations as well as communities.
- *Developing and revising procedures and checklists*: Systematic management of policies involving policy makers and operational personnel for dealing with emergencies and disruptions.
- *Involving the public in Resilience Management*: Communication strategies for crisis management organisations – interacting with the public not yet affected or involved.

INVOLVING END-USERS IN THE CREATION AND EVALUATION OF THE GUIDELINES

The guidelines need to be relevant to actual operations in order to be useful. For this purpose, operational experts representative of potential end-users are involved throughout the project. First, three end-user organizations are part of the project consortium: ENAV, the Italian Air Navigation Service Provider; ISS, the Italian National Health Institute; and KMC, a Swedish center for Disaster Medicine and Traumatology. In addition, members of the DCoP or additional experts from the fields of crisis and resilience management are solicited regularly, for instance: in the modified Delphi process that led to the selection of concepts, approaches and practices to be incorporated in the resilience management guidelines and judgment of their relative importance; in planned pilot studies to support the evaluation of the guidelines. The previous sections have described these experts' inputs in the development efforts, this section will describe their evaluation in greater detail.

The evaluation process is based on three main pillars: (1) an **initial evaluation involving representatives of the end users internal to the DARWIN Consortium**, with experience in HC and ATM domains; (2) the **collection of feedback** from members of the DCoP, including experts of crisis management from a wide variety of domains (not limited to the HC and ATM); (3) the application of the guidelines in a set of **'pilot exercises'** with the active participation of practitioners with experience in the HC and ATM sectors, as well as of experts from different domains which are impacted by the cascading effects of the crisis types identified in the pilot exercises.

(1) The initial evaluation has been performed already. It essentially consisted in two focus group meetings in which a first sample of three Concept Cards was analyzed in collaboration with experts from the three end-user organizations in DARWIN (ENAV and ISS in Italy, KMC in Sweden). The participants of the focus groups reflected on the potential use of the sample concepts cards in their own crisis management activities, providing feedback on their applicability and insights on the opportunities and showstoppers for their implementations in different contexts. Overall, they also helped to better understand the characteristics of the Concept Card format that are more important to develop.

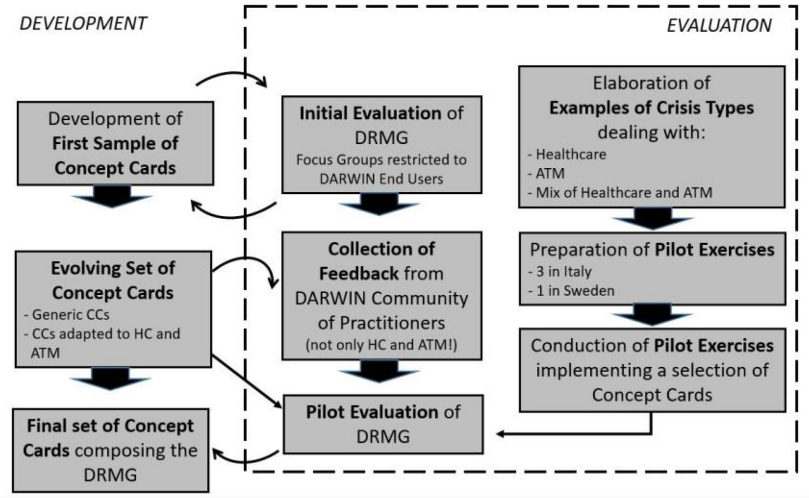


***Figure 1**. Development and evaluation of the DARWIN guidelines.*

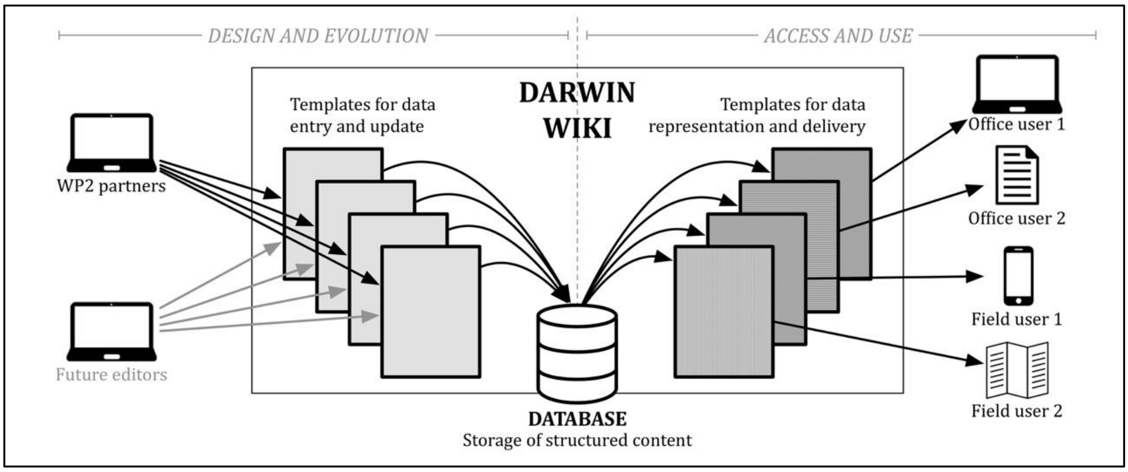
(2) The collection of feedback from outside the project mainly occurred during a workshop organized in March 2017, which was attended by 24 people from the DCoP, belonging to 19 organizations, from 9 different countries. This allowed comparing the experiences of crisis management practices from countries different from Italy and Sweden and from sectors different from the HC and ATM (e.g., water and wastewater networks, civil protection organizations, fire and rescue organizations). In this case, the feedback was less analytical compared to the one achieved during the focus group meetings, but still offered many opportunities to understand how to improve the cards. On the other hand, a larger set of concept cards was available and more aspects of resilience management were addressed.

(3) Finally, the core part of the evaluation will occur during the pilot exercises organized in the second part of 2017 in Italy and Sweden. The pilot exercises consist of different evaluation sessions taking as reference a set of crisis type scenarios identified and designed with the collaboration of the DARWIN end-user representatives mentioned before. Each scenario will be used to investigate the impact of applying the guidelines in real crisis scenarios. Particular importance will be given to crises affecting a mix of the two main domains addressed in DARWIN, but the cascading effects on other domains will also be investigated, with adequate participation of experts from these domains (e.g., fire brigade, civil protection and regional emergency agencies). Four main examples of crisis imagined in concrete contexts have been selected, with particular domain focus (indicated between brackets): Aircraft crashing in urban area close to Rome Fiumicino Airport shortly after taking off (ATM, HC); Blackout in Rome Area Control Centre due to cyber attach (ATM); Disease outbreak during flight due to land at Rome Fiumicino (HC, ATM); Collision between Oil Tanker and Passenger Ferry leaving Gotland Islands in severe weather conditions (HC).

The theoretical approach guiding the evaluation of concept cards is mainly informed by the I-CMO framework (Pawson and Tilley, 1997). This framework is appropriate for formative evaluation of social policies and change programs, and emphasizes the investigation of the conditions (Context) and impact (Mechanisms, Outcome) to understand the fitness for purpose of the Interventions proposed. This evaluation framework is therefore quite relevant to investigate operational issues associated with the implementation of the guidelines developed.

USABLE: SUPPORTING INFORMATION MANAGEMENT AND RETRIEVAL

A key objective of the guidelines is to allow for their flexible use, which corresponds to two different needs: (1) supporting the development and management of the evolving nature of the guidelines, requiring regular revisions of the content; (2) Generating a variety of means to access the guidelines, to account for the variety of envisioned users and uses. These needs correspond to Knowledge Management (KM) issues associated with the storage, versioning, variants, representation, and delivery of content. It quickly appeared that creation of content in typical office documents would constitute a strong limitation to effectively and efficiently update the guidelines as their structure evolve and scope increase, as well as to propose a variety of formats and means to access information. To better fulfil the project KM needs, a wiki-type platform, more specifically based on Semantic MediaWiki, was developed. The DARWIN Wiki provides a standardized way to create content collaboratively, facilitates the management of updates and offers flexible means for delivery of information. The core idea is to separate development of and access to guidelines through structuring the content of the guidelines, content that can then be used in various ways, for instance: reusing content in different formats for different purposes; sorting or aggregating information automatically; creating links between elements.



The main envisioned end-users, e.g., policy makers in a critical infrastructure administration, can consult the

Figure 2. *DARWIN Wiki application: support for development and use of the guidelines.*

guidelines online. Content is organized in four main sections: “Implementation”, “Understanding the context”, “Relevant Material” and “Navigate in the DRMG”. Content related to internal management and review, used for development, is not displayed to end-users. The main information of interest is the “Implementation” section, i.e., the description of the set of interventions proposed for a particular capability. This content, organized by phases of crisis management (across phases, before, during, after), is potentially complemented with “triggering questions”, which aim at pointing users to the relevant issues via a set of questions users can reflect on and try to answer (the use of these questions was inspired by Lay and Branlat, 2014).

For users who would like to better understand the context of the interventions proposed, or refer to original documents describing a method recommended in the CC (sections “Understanding the context” and “Relevant material” respectively), content is available on demand: clicking on the corresponding section title reveals or hide the text. This content access principle is used in other parts of the wiki in order to make the core content more compact and readable (clickable sections or elements are represented by the use of italic text format).

Finally, the “Navigate in the DRMG” section groups in a table the various links that the user can follow to access related DRMG content, e.g., other CCs associated with the same resilience ability, or parent theme.

Following the example of existing guidelines (e.g., WHO, 2008), a “DRMG Field Guide” was created to propose a minimal format to access guidelines outside of the office, i.e. in the field. The Field Guide is not thought of as a complete view of the guidelines, but rather as a quick reference material to remind of and guide people in the field to the right issues, as is the case with a checklist. The assumption for the envisioned use is that access to the guide is possible, whether in real-time online or as a saved document (depending on the constraints). The Field Guide proposed is simply an aggregation of the title, purpose and “triggering questions” for all the existing concept cards, organized by themes.

CONCLUSION

The paper described various issues involved in the development of resilience management guidelines in project DARWIN. Designing useful guidelines (i.e. that will not constitute yet another document sitting on a shelf) requires the consideration of these aspects of development and evaluation, as well as format. During a workshop help in March 2017, participants from different sectors appreciated the general approach and idea of concept cards to address resilience management capabilities. Sessions targeting the implementation of specific guidelines were insightful in various ways, providing input to enrich the current guidelines:

- They provided operational perspectives on the applicability of the interventions proposed, including from organizations and domains outside of the DARWIN end-users;
- They confirmed the needs identified and targeted by the CCs;
- They provided examples of approaches and practices;
- They revealed differences between domains and between countries / cultures.

Relative to the presentation and format of the guidelines, experts insisted on the need to develop focused and easy to understand guidelines. Such feedback will lead to the revision of current guidelines to simplify and clarify the implementations proposed, both through clearer and more focused text, and through identifying opportunities for other forms of content (e.g., generalizing the use of diagrams). However, the project will have to find a reasonable balance between the need for immediate clarity and the potential importance of introducing new concepts or approaches to support resilience management.

Finally, the reception from outside experts was positive on the use of a wiki-type application for resilience management guidelines. It confirmed the general direction taken in the project for providing access to the guidelines and created opportunities to discuss relevant end-user needs that could be investigated before the end of the project (e.g., supporting data collection for resilience assessment). The prototype wiki application[1] offers opportunities to reconsider common views on the nature of guidelines, their necessary evolution, and their multi-faceted, multi-purpose content.

Acknowledgements

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020/2014-2020) under grant agreement n° 653289.

REFERENCES

Adini, B., Cohen, O., Eide, A. W., Nilsson, S., Aharonson-Daniel, L., & Herrera, I. A. (2017). Striving to be resilient: What concepts, approaches and practices should be incorporated in resilience management guidelines? *Technological Forecasting and Social Change*.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management*, *15*(1), 50-59.

DARWIN (2015). Deliverable D1.1. *Consolidation of resilience concepts and practices for crisis management*.[2]

DARWIN (2016). Deliverable D1.3. *Practitioner and academic requirements for resilience management guidelines*.[2]

DARWIN (2017). Deliverable D2.1. *Generic Resilience Management Guidelines*.[2]

Herrera, I., Woltjer, R., Branlat, M., Nevhage, B. (in press). Dealing with crises in critical infrastructures: risk and resilience as complementary management approaches. *Proceedings of ESREL 2017*.

Lay, E., & Branlat, M. (2014). Noticing Brittleness, Designing for Resilience. In C. P. Nemeth & E. Hollnagel (Eds.), Resilience Engineering in Practice: the Road to Resilience. Farnham, UK: Ashgate.

Pawson, R., & Tilley, N. (1997). *Realistic Evaluation*. London, UK: Sage.

WHO (2008). Guidelines on Mental Health and Psychosocial Support in Emergency Settings: checklist for field use. World Health Organization – Inter-Agency Standing Committee (WHO-IASC). Available at: http://www.who.int/mental_health/publications/check_list_IASC_guidelines/en/, accessed 2017-04-06

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, *141*, 5-9.

Woods, D. D., & Branlat, M. (2011). Basic patterns in how adaptive systems fail. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), Resilience Engineering in Practice: A Guidebook (pp. 127–143).

[1] Available at: http://sintef9013.com/darwin_wiki/

[2] Available at: http://www.h2020darwin.eu/project-deliverables

FOCUS ON SUCCESS: A SAFETY-II APPROACH ON OPERATIONAL MANEUVERS IN THE ITAIPU BINACIONAL HYDROPOWER PLANT

Juliano Couto Portela[1] and Lia Buarque de Macedo Guimarães[2]

[1] Universidade Federal do Rio Grande do Sul, Av Osvaldo Aranha, 99, Porto Alegre, Brazil

[1] jportela@itaipu.gov.br

[2] Universidade Federal do Rio Grande do Sul, Av Osvaldo Aranha, 99, Porto Alegre, Brazil

[2] liabmg@gmail.com

Abstract

Accidents in critical infrastructures, such as the Itaipu Binacional HPP, although rare, cause serious social and economic impacts in their area of influence. Therefore, they must be avoided even if a "normal" accident rate is expected due to the operation complexity. This paper investigates the conditions leading to operational failures in the Itaipu operation under the approach of Safety-II management related to Resilience Engineering, "in the many things go right", contrasting the Safety-I view, based on the retrospective analysis and "the few things went wrong". Guided by the structured opinions of the operational staff and inspired by the FRAM method, the study deals with the normal operation and variabilities of four typical operational maneuvers within the quadrants of a periodicity-complexity matrix. The results indicated that the same variabilities influence the operation regardless of the complexity or periodicity of the maneuver. A comparison between the analysis of the variabilities in a typical situation and the four operational failures occurred between 2006-2015 indicated that some variabilities act decisively in virtually all maneuvers. The results were discussed with the team members who proposed the adaptations to increase the operational safety of normal work.

INTRODUCTION

Accidents of big proportions in organizations of high sociotechnical complexity cause great social and economic impact. Chernobyl, (1986), Three Mile Island (1979), Sayano-Shushenskaya (2009), Fukushima (2011) and Deepwater Horizon (2010) are examples. In all, the variabilities that affected the operational process had become out of control, impacted vital functions of the process, and eventually lead to the fatal failures. In situations of minor failures, as in industry or health service, the reason for accidents normally is understood by the use of techniques that search for contributing factors to the damage, focusing on “what goes wrong” in an approach known as "Safety-I".

Even if subsequent analysis had been successful in pointing out the root causes of these accidents and established new safety standards, it’s clear that if the conditions that led to the accidents had been anticipated, they probably had been avoided. Achieving it requires a different approach to normal operation and a different way of thinking about safety. Rather than reactive, it should be proactive: perceiving the hazards of the process before they get out of control. This new approach, called "Safety-II", considers important focusing on adaptive capacity in order to maintain control over unforeseen disturbances or events (Lundberg & Johansson, 2015). In addition, security should not focus on the rare cases of failures because they do not explain why performance is almost always satisfactory and how it helps to meet organizational goals.

Itaipu Binacional has 14,000MW of installed power. It is the largest power generator of the world, having produced nearly 2.5 billion MWh since 1984. It is responsible for 17% of the Brazilian’s energy consumption and 75% of the Paraguayan’s. Therefore, shutdowns at Itaipu Binacional have the potential to cause loss of production and instability to both electrical systems. Thus, it is for the best interest of the societies that the organization assumes the proactive view provided by Safety-II guidelines. Based on the principle of equivalence between "successes" and "failures", this view assumes that both normal operation and accidents emerge from the same origin. By this approach, safety is a consequence of the way the complex system behaves, not a static property. Furthermore, adopting Safety-II practices meets the vision of sustainable production and high operational performance, represented by a sequence of world records of energy production, the last one achieved in 2016 (more than 103 million of MWh). This article presents the method used to address the “focus on success” in the Itaipu operation by analysing four maneuvers that represent the universe of maneuvers in a periodicity-complexity matrix. Next, it traces the normal operation of such maneuvers, the variabilities that influence each step of the chosen maneuvers, and then evaluates the impact of each maneuver step on the overall result (success or error). Finally, analyses the failures already occurred to verify the adherence of the study to the situations already experienced.

SAFETY-I AND SAFETY-II

By understanding safety as an absence of unwanted results in normal operation, the goal of the "traditional" safety management – Safety-I – is to maintain a safe condition where the number of unwanted outcomes is as small as possible (Eurocontrol, 2013). "New" accidents occur because their cause was not eliminated as it was unknown. Technological upgrades, changes in human or organizational resources can bring new causes (Patterson, Deutsch, 2015).

Safety-I thus promote a bimodal way of seeing work and activities: when how things work out is because the system works as it should and because as people work in the prescribed way, as one imagines; When they go wrong, it's because something goes wrong or it fails. Security is a quality that the system is sufficient to ensure that the number of potentially harmful events (Eurocontrol, 2013).

Hollnagel (Vanderhaegen, 2015), by explaining there is a distinction between the Work-As-Done and Work-As-Imagined, where the latter is generally considered in a Safety-I approach, considers a mistake thinking of human beings as machines capable of responding in infinite ways to infinite possibilities. In short, in the approach of Safety-I mainly refers to the evaluation of the lack of security rather than the presence of security. However, the number of failures or accidents is much smaller than the number of successes in normal operation. In fact, Figure 1 shows the number of well-succeeded operational maneuvers selected for the study performed by the Itaipu operation in the period 2006-2015 and the failures resulting in loss of energy production, reliability or damage to equipment during that time. It can be observed that the failures represent 0.025% of the universe, while the successful maneuvers represent 99.975%. This is adherent to what is shown in (Eurocontrol, 2013).

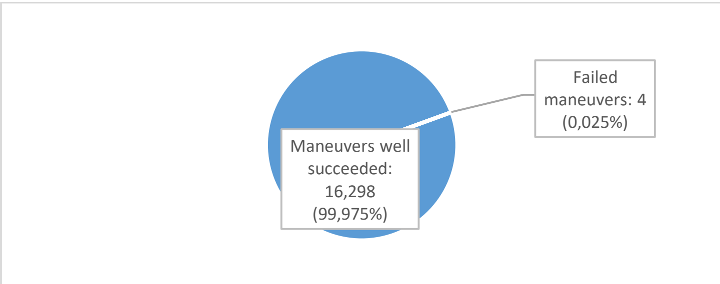


Figure 3 *Well-succeeded x failed maneuvers considered in the study between 2006-2015*

The contemporary security approach, called Security-II, is based on the principle of equivalence between successes and failures as well as fine-tuning performance, which makes performance always variable. Even in a normal operation, a certain variability can propagate from function to function, ultimately leading to an unexpected result, or non-linear effects (Hollnagel et al, 2015). Therefore, both normal operations and eventual accidents emerge from functions whose results are influenced by the variabilities present in any successful or failed operation. The extent of such variabilities (and their monitoring) is that will define the operation outcome. Security is, therefore, an emergent property that involves the operation of a complex system being a consequence of the way the system behaves, not a static property.

In short, Safety-II is based on a simple principle: one must understand and support the much that works (Patterson, Deutsch, 2015) instead of investing effort and resources in the few occasions when things go wrong. Focusing on success instead of focusing on failure implies that human actions are performed on real situations, subjected to high variability. According to this view, one must avoid treating failures as unique events, but see them as the expression of the variability of performance in the daily routine. Things that went wrong have worked well many times before, and will work out many other times in the future. In other words, when the error occurs, one should begin by understanding why the action is usually correct rather than looking for specific explanations to the failure (Hollnagel et al, 2015).

METHOD

Although safety management according to the precepts of Safety-II is still incipient, there are methods that can present an approach to the "focus on success". None of them, however, is specific to Safety-II. They are approaches that can be adapted to reach this goal in at least one criterion (Eurocontrol, 2013).

Reviewing some of the methods (Eurocontrol, 2013), the FRAM was chosen to serve as an inspiration for the study from a conceptual point of view, for it reflects the view of Safety-II and Resilience Engineering (Hollnagel et al, 2014). Inspired by the FRAM, the study mapped the functions of typical maneuvers of the Itaipu Binacional operation, their variabilities, and interfering conditions on normal operation.

Due to the significant number of maneuvers executed by the Itaipu operational team, each one with several steps with different levels of complexity and attention, a matrix of four quadrants was created with categories "complexity" and "periodicity", where four maneuvers represent the universe for the purpose of this study. The periodicity refers to the number of times the maneuver was performed during the period. The complexity refers to the number of steps to be taken and the number of factors (vulnerabilities/noises) to influence its success. One of the criteria for choosing the maneuver was that it should cause an impact on the energy production or safety of human resources, facilities or the surroundings of the plant if unsuccessful.

In order to: - choose the maneuvers representing the four quadrants of the periodicity-complexity matrix; - determine the variabilities that influence each step of the chosen maneuvers; - evaluate the impact of each step of the maneuver on the overall result – success or failure –, interviews were conducted with 31 technicians and 8 engineers of the operation team. The results are shown in the Table 1.

Table 1. *Maneuvers considered in the study – period 2006-2015*

Maneuver	**Periodicity**	**Complexity**	**Total of maneuvers**
Select generating units to conventional control	LOW	LOW	553
Separation of generating units for ANDE	LOW	HIGH	27
Reversal of speed regulator pumps	HIGH	LOW	10,400
Start and stop of generating unit	HIGH	HIGH	5,322
TOTAL			**16,302**

RESULTS AND DISCUSSION

Variabilities

The variabilities that influence these four operational maneuvers were also obtained through the interviews with the professionals. It was verified that, regardless of the complexity and periodicity of the maneuver, 16 variabilities, grouped into 6 categories, are common to the four types of maneuvers, as shown in Table 2.

Table 2. *Variabilities that influence the operation*

Category	**Variability**
Operator	Knowledge/experience
	Ability to adapt to unexpected situations
	Necessity to confirm each step with another operator
Communication	Communication equipment availability
	Operator/Supervisor reports each step
	Quality of operational communication (eg. clear and objective communication between O&M)
Human Resources	Availability of human resources
	Hierarchy in the execution of step
Operational Instruction	Quality of the operational instruction
	Current operational restrictions
Maneuver Environment	Situations that take the operator's attention (e.g. telephone/alarm)
	Urgent / emergency situations or concomitant work
	Similarity with another maneuver environment
Maneuver equipment	Normal operation of the maneuver equipment
	Availability of the computerized systems
	Tacit peculiarities of the equipment (not described in any instructions)

From the start to the end of the maneuver, several steps are performed. For the purpose of the study, there are two types of steps: 1) *Key step*: central function from which the purpose of the maneuver is achieved. An error in a key step most probably causes an error in the maneuver itself. Examples: breaker closure, unit synchronization. It is similar to the *functional resonance* of the FRAM method; 2) *Relevant step*: although it is not a key step, it contributes to the normal flow of the maneuver in a decisive way; a failure in this step can influence the key step, and therefore cause error in the maneuver. Examples: trigger starting preparation, confirm voltage bar without voltage before switch closure;

Table 3 shows the 7 steps of one of the maneuvers (Select generating units to conventional control) with some of the variabilities – see Category "Operator" in Table 2 – to illustrate how the general table was assembled. It was considered less important to understand the technical meaning of each step than to understand how each variability influences each step. The "X" implies that the variability influences the step.

Table 3. *Example of maneuver steps and variabilities*

	Maneuver step	Key step (functional resonance)?	Operator – Knowledge/ experience	Operator - Ability to adapt to unexpected situations	Operator - Necessity to confirm each step with another operator
1	Request to the dispatch center to turn off the Automatic Control of Generation	N			
2	Set reference power in the Turbine Joint Control	S	X	X	X
3	Confirm that the voltage value is zero in the Joint Control	S			
4	Set reference voltage in the Voltage Joint Control	S	X	X	
5	Select generating units, transmission lines and voltage bars from Scada 1 to conventional	S	X	X	X
6	Confirm the switch key 43JCS in the Joint Control in the "conventional" position	N			
7	Switch generating units on conventional panel to the same position as in the digital system	N	X	X	

For example, it was considered that the "Operator Knowledge" variability does not influence the "Request to the dispatch center to turn off the Automatic Control of Generation" step, as the knowledge is not relevant to the outcome of this step. On the other hand, it was considered that "Ability to adapt to unexpected situations" influences the "Set reference voltage in the Voltage Joint Control" step because, if there is an unexpected situation at the time of this maneuver - for example, disturbance in the electrical system - the Operator must be able to adapt the maneuver to this situation.

Based on the evaluation of the operation team, the question "which variabilities in Table 2 influence this step?" was asked for each of the steps. The overall result is shown in Table 4, which gives an overview of the specific variabilities for each of the four quadrants of the matrix complexity-periodicity.

Table 4. *Variability frequencies on the maneuver key steps*

LOW COMPLEXITY		HIGH COMPLEXITY	
Maneuver environment – Similarity with another maneuver environment	85 %	Maneuver environment – Urgent / emergency situations or concomitant work	76 %
Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	62 %	Maneuver equipment – Normal operation of the maneuver equipment	74 %
Instruction – Current operational restrictions	62 %	Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	74 %
Instruction – Quality of the operational	54	Human Resources – Availability of human	67
Operator – Knowledge / experience	46	Operator – Necessity to confirm each step with	64
Operator – Ability to adapt to unexpected	46	Instruction – Current operational restrictions	64
LOW PERIODICITY		**HIGH PERIODICITY**	
Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	93 %	Maneuver equipment – Normal operation of the maneuver equipment	61 %
Human Resources – Availability of human	85	Operator – Knowledge / experience	57
Instruction – Quality of the operational instruction	85 %	Maneuver environment – Similarity with another maneuver environment	57 %
Operator – Necessity to confirm each step with another operator	81 %	Maneuver environment – Urgent / emergency situations or concomitant work	50 %

Instruction – Current operational restrictions	78 %		Maneuver environment – Situations that take the operator's attention (e.g. telephone/alarm)	50 %
Maneuver environment – Similarity with another maneuver environment	74 %		Instruction – Current operational restrictions	50 %

From Table 4, we can draw some conclusions:

a) The "maneuver environment" is significant in all situations of complexity and periodicity;
b) The “knowledge/experience”, despite its central importance, does not appear as a main variability in the maneuvers of high complexity and low periodicity;
c) Most of the steps are affected by "Similarity with another maneuver environment "; it is usual in plants with several generating units that each environment where the operator performs the maneuver is exactly equal as the adjacent, except for the operational identifications;
d) The category "instruction" affects significantly the low complexity and low frequency maneuvers;
e) In the case of low periodicity maneuvers, many of the variabilities affect almost all the steps. The main variability is the “Situations that take the operator's attention”. This is because as the maneuver is rarely executed, the operator tends to turn all the attention to the execution, and all the attention-taking conditions influence the normal operation;
f) In maneuvers of high complexity, the two variabilities that most affect the functions ("Maneuver environment - Urgent / emergency situations or concomitant work" and "Normal operation of the maneuver equipment") are external variabilities, so the operation has no much to do as a concrete action to decrease their influence on the maneuver, but emphasize the importance of the experience as well as the knowledge management as a way to increase the operation capacity of adaptation and response to eventual disruption, one of the primal precepts of RE.

Comparison between the variabilities raised and actual failures

Although Safety-II emphasized the analysis of success rather than failures, it was understood important to confront the results obtained with the four operational failures occurred between 2006 and 2015. The variabilities that influenced each one are summarized in Table 5.

The first operational process failure, occurred in 2010, was made in a maneuver of low complexity and high periodicity. The analysis indicated process failures in 5 out of 6 steps. There was a coincidence between the activation of an alarm and an unrelated work on the equipment, where the latter required special attention of the operator. When analysing the alarm in front of the equipment, the operator missed the comprehensive understanding of the operational situation, performing an undesired maneuver of pump transfer.

Second failure, occurred in 2008, was made in a maneuver of high complexity and low periodicity. The analysis indicated process failures in 2 out of 17 steps. In the occasion, the generating unit U9A should be switched off for maintenance. However, at the same time, the dispatcher asked to shut down the U03 along with the U9A in order to meet electrical systems demands. Upon entering the digital system screen to open the U9A circuit breakers, the operator was induced by the information that U03 should be also stopped. Thus, mistakenly the operator accessed the control panel of the U03 instead of the U9A and opened the circuit breakers with U03 still at full power, causing load rejection in the U03.

Third failure, occurred in 2014, was made in a maneuver of high complexity and high periodicity. In this, failure was found in 3 of the 22 steps. The generating unit U09 should start and synchronize to the electrical system. In order to run the start-up sequence automatically, it would be necessary for an operator be locally on the unit’s local control panel to switch the control mode to automatic. Since the local operator wasn’t found, the operator in the Control Room decided to perform the maneuver even so. With concomitant work in progress in the control room, the maneuver was performed by a single operator. In this process, the U09 circuit-breaker was closed out of ideal synchronization conditions, resulting in mechanical and electrical damage to the unit.

Fourth failure, occurred in 2014, was made in a maneuver of high complexity and high periodicity. In this, failure was found in 3 of the 22 steps. During the stopping process of generating unit U05 to meet electrical system requirements, the operator mistakenly transferred the power supply selection of the unit U04 instead of U05. It was necessary to stop the U04, which was operating normally at the time.

Without taking the frequencies into account, Table 5 shows the variabilities that influenced the four operational process failures between 2006 and 2015.

Table 5. *Summary of the variabilities that influenced the four failures*

Failure 1: 2010 occurrence **(Low complex/High periodic)**	***Failure 2: 2008 occurrence*** **(High complex/Low periodic)**	***Failure 3: 1st 2014 occurrence*** **(High complex/High periodic)**	***Failure 4:2nd 2014 occurrence*** **(High complex/High periodic)**
Maneuver environment *– Situations that take the operator's attention (e.g. telephone/alarm)*			
Maneuver environment *– Urgent / emergency situations or concomitant work*		***Maneuver environment*** *– Urgent / emergency situations or concomitant work*	
	Maneuver environment *– Similarity with another maneuver environment*		***Maneuver environment*** *– Similarity with another maneuver environment*
	Operator *– Necessity to confirm each step with another operator*	***Operator*** *– Necessity to confirm each step with another operator*	***Operator*** *– Necessity to confirm each step with another operator*
Operator *– Knowledge / experience*			
Maneuver equipment *– Normal operation of the maneuver equipment*	***Maneuver equipment*** *– Normal operation of the maneuver equipment*	***Maneuver equipment*** *– Normal operation of the maneuver equipment*	
		Human Resources *– Availability of human resources*	

Although totally different in circumstantial terms, some similarities that corroborate conclusions drawn from Table 4 can be noted:

a) The "maneuver environment" is important in all situations of complexity and periodicity;

b) The "operator knowledge" is not a main variability to influence maneuvers of high complexity and low periodicity. In fact, the reports pointed out that in the cases of faults 2, 3 and 4 the operators were fully aware of the operational procedure;

c) Most of the steps are affected by the variability "Similarity with another maneuver environment". In the case in question, in two of the four failures it was present;

d) The category "instruction" affects more significantly the low complexity / periodicity maneuvers.

e) In low periodicity maneuvers, many variabilities affect practically all steps. The main variability affecting normal operation comes from situations that get the attention of the operator.

f) The analysis of the reports has proved that malfunctioning of the maneuvering equipment and concomitant emergency / work situations are basic failure conditions. The operation should maintain the priority of its knowledge management systems and training to decrease their influence on the results of the maneuvers.

FINAL CONSIDERATIONS

This study applied precepts of Safety-II in a set of four maneuvers categorized in high and low complexity and periodicity performed by the operation of the Itaipu Binacional HPP, inspired by the FRAM method, in order to understand which variabilities influence the normal operation. Maneuvers were detailed in steps; for each, it was pointed the variabilities that act on them and it was concluded which variability most influences the normal operation. By this, variabilities that influence the operation are common to all studied maneuvers.

The results were compared to the reports of the four operational process failures occurred between 2006 and 2015. The conclusion is that although it is fragile to say that the four maneuvers represent the whole universe of more than five hundred maneuvers executed by the Itaipu operation, they provide valuable inputs to the study by allowing pertinent conclusions comparing what was verified in the study with the actual cases of failure. Some of that are: a) some variables act decisively in practically all maneuvers. Among them, the category maneuver environment, the need to confirm the steps of the maneuver with another operator, situations that draw attention from the operator and the similarity with another operating environment. The operator knowledge was not mapped as a fundamental variability present in the failures.

Comparisons between normal operation and failure cases proved success and failure come from the same source, which is adherent of the Resilience Engineering principles. Once identified the maneuver functions, it was possible to understand which would be the most important variabilities that influence normal operation, providing subsidies to the organization to the decision-taking before an event of failure.

The main contributions of this work for the development of the discipline are:

a) The confirmation that the same variabilities influence the operational steps, regardless of the complexity of the periodicity of the maneuver.

b) The reports of the four failures corroborated fundamental aspects of the study;

c) The Resilience Engineering and Safety-II approaches are adherent to the real cases found.

REFERENCES

M. Patterson and E. S. Deutsch, “Safety-I, Safety-II and Resilience Engineering,” Curr. Probl. Pediatr. Adolesc. Health Care, vol. 45, no. 12, pp. 382–389, 2015.

J. Lundberg and B. J. E. Johansson, “Systemic resilience model,” Reliab. Eng. Syst. Saf., vol. 141, pp. 22–32, 2015.

EUROCONTROL, “From Safety-I to Safety-II: A White Paper,” Netw. Manag., pp. 1–32, 2013.

F. Vanderhaegen, “Erik Hollnagel: Safety-I and Safety-II, the past and future of safety management,” Cogn. Technol. Work, vol. 17, no. 3, pp. 461–464, 2015.

E. Hollnagel, R. L. Wears, and J. Braithwaite, “From Safety-I to Safety-II: A White Paper,” Netw. Manag., p. 43, 2015.

E. Hollnagel, J. Hounsgaard, and L. Colligan, FRAM – the Functional Resonance Analysis Method - A handbook for the practical use of the method, 1st ed., no. june. Middelfart, Denmark, 2014.

STUDY OF A SAFETY AND SECURITY FRAMEWORK BASED ON RESILIENCE ENGINEERING

Nyambayar Davaadorj [1] and Ichiro Koshijima [2]

[1,2] Department of Architecture Civil Engineering, Nagoya Institute of Technology, Gokiso-Cho, Showa-Ku, Nagoya City, Japan

[1] cjv18504@ict.nitech.ac.jp

[2] koshijima.ichiro@nitech.ac.jp

Abstract

Manufacturers are subject to legal requirements for protecting the health and safety of the personnel inside and around the workplace and of those who are directly exposed to workplace activities. Although it might be difficult to manage a situation in which complete safety is ensured, efforts must be made to consider the ways of removing and mitigating potential hazards. Recently, based on the rapid development of IT applications, manufacturers are additionally charged with identifying cybersecurity hazards within the production environment as well as ensuring employee safety. So far, safety and security have been addressed separately within the IT security and production-safety domains, respectively. However, rapidly developing IT and network technologies have made sophisticated cyberattacks widely possible. Hence, there exists a practical need for simultaneously achieving industrial safety and security in the workplace.

In this research, a proactive analysis based on IEC 62443 (internationally applied standard for the manufacturers and operation of industrial management security) and occupational safety and health management system (OSHMS) is proposed. We present a methodology based on a global standard for combining the safety and security operations to maximize resiliency against a potential cyberattack scenario.

1. INTRODUCTION

Chemical manufacturers are subject to legal requirements for protecting the health and safety of the personnel who are inside and around the workplace and of those who are directly exposed to workplace activities. Although it might be difficult to manage a situation wherein a complete level of safety is ensured, efforts must be made to consider ways of removing potential dangers to workforces within an organizational setting. Such an organization should therefore perform a programmatic-level risk assessment for understanding the specific hazards that may exist within their specific processing areas. After the risk assessment, the organization should summarize the discovered information and then communicate it to downstream importers, distributors, and customers. Moreover, the organization should ensure that viable safety and security risks are determined and controlled. The term “safety” refers to a state of being “safe,” whereas production hazards are recognized and controlled to an acceptable level.

Based on the rapidly developing IT technologies, manufacturers are continually charged with identifying hazards related to cybersecurity and employee safety. The term “security” in the production field pertains to the risk created by cyberattacks to an industrial control system (ICS). ICSs are typically employed in industries when connections to the internet are made for data analysis purposes. So far, safety and security have generally been addressed as separate tenets within the IT security and production safety domains. However, the rapidly developing IT and network technologies, have made sophisticated cyberattacks a real possibility. A cyberattack is a huge risk for the safety and security of production processes; therefore, there is a practical need for embracing simultaneous achievement of safety and security from a business continuity standpoint.

In this research, a discussion is set forth based on the global standards for safety and security, which refer to IDEF0 for function modeling [National Institute of Standards and Technology, 1993] and the derived organizational matrix (referred to as the “resilience matrix”) presented within. The global standard for security is IEC 62443 (internationally applied standard for the manufacturers and operation of industrial management security) [IEC Central Office, 2010], while the global standard for safety is the occupational safety and health management system (OSHMS), an internationally applied standard that has been notably implemented for reducing potential risks within production/processing facilities [OHSAS Project Group, 2007]. Finally, this research discusses a methodology for combining the safety and security aspects to maximize resiliency levels against potential cyberattacks.

2. ANALYSIS OF GLOBAL STANDARD FOR SAFETY AND SECURITY

2.1 Setting up the issue from the global standard

For simultaneously achieving safety and security, an analysis is required to accurately characterize both the safety and security standards. For the safety standard, the OSHMS has previously been assessed [Davaadorj Nyambayar, 2016].

For the security standard, IEC 62443 has been previously analyzed by a worldwide organization for standardization, which comprises all national electrotechnical committees [IEC Central Office, 2010].

In both these analyses, the global standard(s) pose the following queries/issues when a structure of each activity is set up and evaluated with regard to industrial system resiliency within each organization:

1. Clarification of activities in standard clauses: Based on the safety and security standard clauses, are the actions which should be performed, the order in which such actions are performed, and the considerations to be taken into account for the actions clearly provided?
2. Determination of other actions inherent to the standard process: Are the determined actions that should be performed clearly provided even though they are not sufficiently detailed in the standard clauses?
3. Considering a methodology to determine how a corporation might use an organizational structure to provide safety and security for a business continuity environment.

2.2 Analysis method of risk identification

For each section, global standard risk assessment is discussed and analyzed. All assessed examples in this section consider only risk identification, classification, and assessment, which contain directives on main activities for responding to safety and security. The analysis of global standards was conducted by deconstructing and categorizing the clauses with the following configurations:

4. The main activities in the sentences (for extracting only the sections of recommendations for actions related to the system risk assessment for safety and security)
5. Subjects within the sentences
6. Objects and verbs within the sentences
7. Knowledge, skills, and rules

The result showed that the entity in charge of the risk assessment activity is primarily the “organization,” and there is no mention in the standard of “who” should actually “implement” the activities. Furthermore, when the object was extracted during the analysis, very few details were actually mentioned. It was hence not clear what actions should be performed within the organization. The global standard is rule-based. There are many rules inclusive within the safety and security standards. Under these rules, methods and knowledge of other skills are clearly necessary. However, such facets prove difficult within a foreign industrial company’s attempt to adopt a global standard with a built-in continuous improvement process due to considerable misunderstanding. According to a previous study [Rasmussen J, 1983], discussions are presented regarding requirements at the skill-, rule-, and knowledge-based levels, along with a review of the different levels associated with signals, signs, and symbols. Rasmussen remarked “When we distinguish categories of human behavior according to basically different ways of representing the constraints in the behavior of a deterministic environment or system, three typical levels of performance emerge: skill-based behavior, rule-based behavior, and knowledge-based performance.”

2.3 Clarification of activities in global standard clauses

When a corporation implements the global standard, it follows the relevant clauses in the safety and security standard. The standard uses the main requirement in a plan–do–check (evaluate)–act (review and implementation) (PDCA) structure, which includes policies, goals, safety and security goal planning, its implementation and operation, daily inspections and improvements, record updates, and regular reviews of the system itself. This system of business management is adopted by corporations due to its basic principle of improvement in each cycle, which is caused by traversing the PDCA motions. The safety and security standards require the update of vulnerability assessment records; however, there is no mention of continuous improvement strategies in the literature. Consequently, three areas were resultantly uncovered wherein information is unclear in the implementation and operation of the global standard:

1. The input and output of a given activity

2. The main responsibilities of a person who performs the activity
3. The conditions on the limitations and resources that must be considered for the execution of the activity

For example, to identify these elements in the clauses of the OSHMS standard, an IDEF0 modeling methodology is used.

The activity in IDEF0 can be identified as the verbs in the standard clauses of the OSHMS. Concomitantly, whatever is fed to execute this activity is expressed as the input and the results of executing the input through the activity can be expressed as the output. The control is implemented by a limiting condition in executing the activity, and a mechanism is formed in a manner in which the execution of the activity is supported. This is expressed as the resource (particularly the executor of the activity) to execute the activity.

Figure 1 shows the determination of the source of a hazard, a risk assessment, and a decision-making process-flow for an exercised management method based upon the clauses in the risk assessment section of the OSHMS standard. The existing activities are a determination of the source of the hazard and risk assessment and the establishment of steps to determine how to manage, implement, and update the records disseminating those steps.

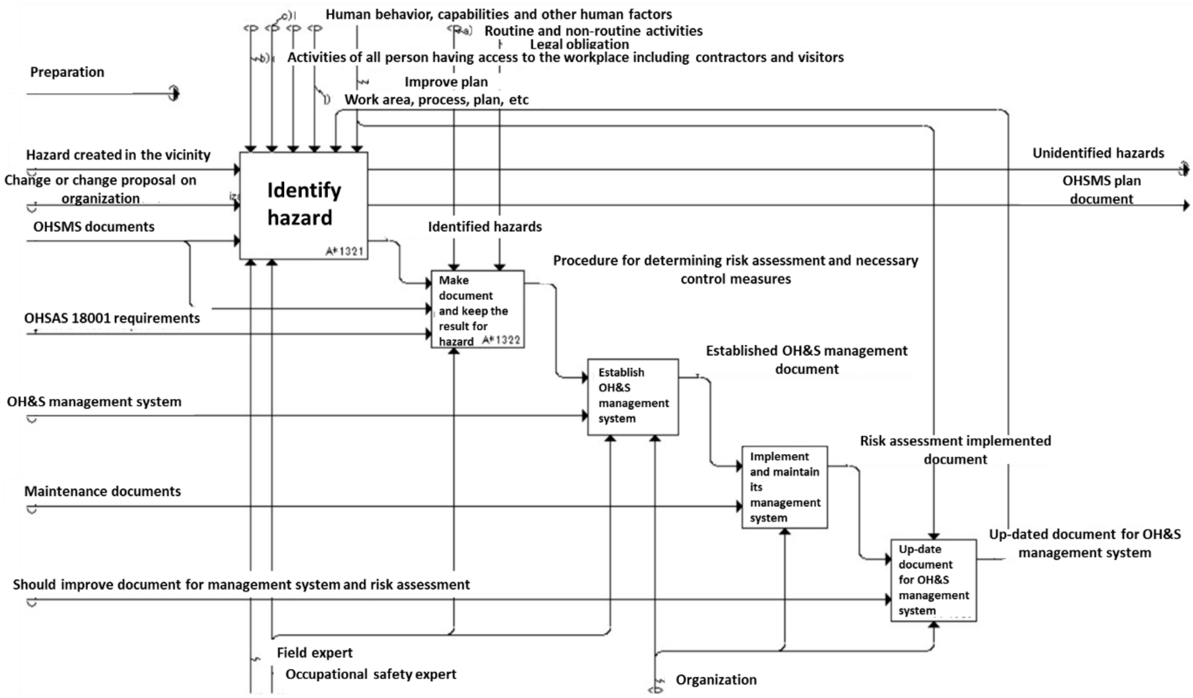


Figure 1. *IDEF0 modeling of the occupational safety and health management system (OSHMS) risk assessment*

3. OPERATION OF RESILIENCE MATRIX

The model of the global standard expressed through the use of IDEF0 is transformed into a resilience matrix (RM) to determine inherent activities. The RM describes a model whose capacity to respond (i.e., resilience) to signals is considered in the context of an organization. The RM is a 3 × 3 matrix comprising nine cells, with the horizontal axis representing the response provider (i.e., individual, group, and organization) to the signals and the vertical axis representing the ease with which the signals change (in three stages from low to high). Each of the nine cells shows that a certain response provider should perform a specific action to enhance resilience within an organization in response to varying signals. In this matrix, Rasmussen's skill–rule–knowledge (SRK) model and organizational levels (i.e., individual, group, and organization) are combined in the 3 × 3 chart.

3.1 Results of the RM OSHMS model

The results of the analysis are projected onto the RM. The RM can be defined as a cycle mechanism to develop new operational procedures so that an individual can implement them and provide feedback regarding their ease of use to maintain and increase organizational resilience. Accordingly, it seems appropriate to place the IDEF0 model of the OSHMS standard into the RM to specify the structure of the organizational activity cycle and identify inherent activities.

Figure 2 shows the OSHMS risk assessment clauses expressed in the IDEF0 model and transferred to the RM as well as the relevant inherent activities. The activities in the box cells pertain to the OSHMS clauses according to the RM. With the representation of the IDEF0 version of the OSHMS clauses, the “establishment of procedures” by an “organization” is connected to the inputs and outputs through the “implementation of the procedure” by an “individual.”

Figure 2 shows the PDCA cycle for the OSHMS standard. The PDCA cycle ultimately aids in the dissemination of the OSHMS standard throughout the example organization. To execute this company-wide PDCA cycle continuously without failure, it is necessary to establish a section-based PDCA cycle at each stage of the cycle within the individual, group, and organizational levels.

In an organizational structure with a section-based PDCA cycle,

- • Each section goes through the implementation, maintenance, and improvement processes.
- • Subsequently, the improvement must be checked and tested. If it passes the check, one can proceed to the next stage.
- • If the improvement fails the check, one goes back to an improvement process, provide safety instructions, and then return to the cycle.
- • This is repeated in each responding section of the organization.

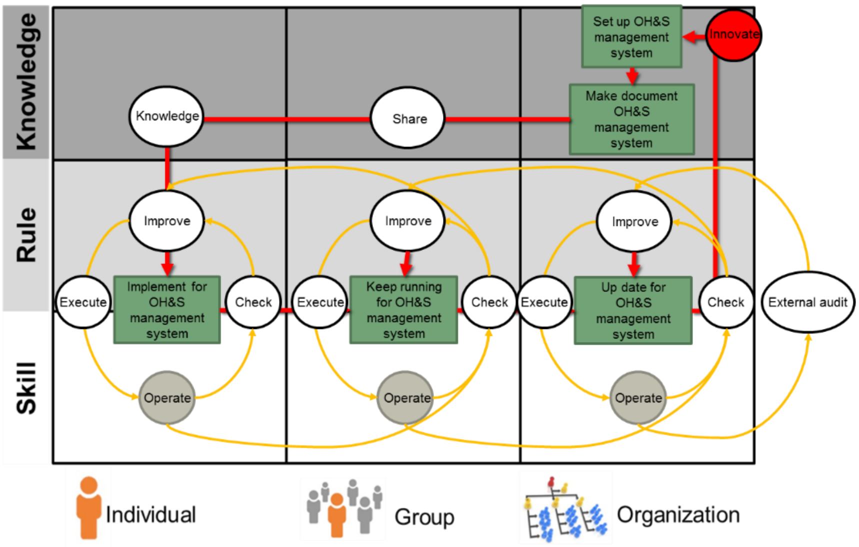


Figure 2. *Resilience matrix (RM) for the OSHMS based on the IDEF0 diagram*

3.2 Results of the RM-IEC 62443 model

The analysis results of IEC 62443 were projected onto the RM. The RM can be defined as a cycle mechanism for developing new operational procedures, for an individual to implement them, or to provide feedback regarding their ease of use to maintain and increase organizational resilience for the IEC 62443. Accordingly, it seems appropriate to place the IDEF0 model of the IEC 62443 standard into the RM to specify the structure of the organizational activity cycle and identify inherent activities. Figure 3 shows the IEC 62443 risk assessment clauses expressed in the IDEF0 and transferred to the RM as well as the relevant inherent activities. The activities in all steps pertain to the IEC 62443 clauses. In particular, the activities in “Conduct risk assessment throughout the life-cycle of the IACS,” “Document the risk assessment,” and “Maintain vulnerability assessment record” constitute the main PDCA cycles for the IEC 62443 clauses. The representation of the activities selects a risk assessment and identifies the IACS based on the “organization,” which is connected to provide risk assessment information, including methodology training. The activities in the “Prioritize system,” “Conduct a detailed risk assessment,” and “Identify the reassessment frequency and triggering criteria” sections follow the rule-based activities. Based on these facets, it can be assumed that a resilient organizational model should appear similar to that (should be similar to the RM-OSHMS model) depicted in Figure 3. The PDCA cycle helps disseminating the IEC 62443 standard throughout the example organization. To execute this company-wide PDCA cycle continuously without failure, it is necessary to implement a section-based PDCA cycle at each stage of the cycle. Figure 3 shows where it is possible to establish this PDCA cycle within the individual, group, and corporate levels.

In an organizational structure with a section-based PDCA cycle:

- • Each section goes through the life cycle of the IACS, documents the risk assessment, and maintains vulnerability assessment records and improvement measures.
- • Subsequently, the improvement should be checked and tested. If it passes the check, one can proceed to the next stage.
- • If the improvement fails the check, one goes back to the improvement process, provide safety instructions, and then return to the cycle.
- • PDCA is repeated in each responding section of the organization.
-

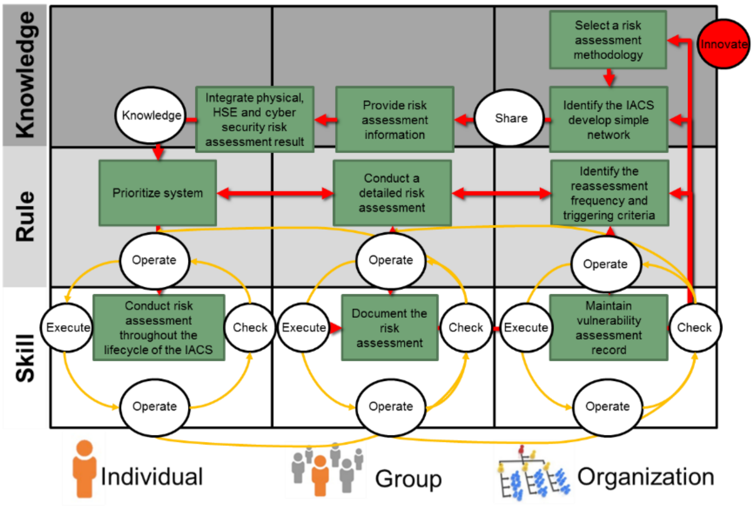


Figure 3. *RM for IEC 62443 based on the IDEF0 diagram*

4. SAFETY AND SECURITY MANAGEMENT FRAMEWORK

An ICS is typically used in industries and in manufacturing, and it conventionally connects the Internet with big data to analyze an appropriate way to improve a production process. The ICS hence presents numerous benefits to consumers and has the potential to enhance the ways in which consumers ultimately interact with each other via technology. However, the ICS is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend, particularly from the security and safety standpoints. As physical objects, dangerous risks to factory workforces inherently exist from regular equipment use and other potential sources.

The reason why it is important to identify ways of successfully integrating the security and safety requirements is that during a cyber incident, there are constraints on an organization (e.g., knowledge limitations and human resources) and the environment (e.g., resources and systems) targeted for the response. In addition, there are time constraints incumbent upon the emergency system during a cyber incident. Figure 4 shows the relationships between safety and security corresponding to a given resource. Since cyberattacks may cause unsafe conditions in control systems, safety measures are a top priority for implementation.

In the course of a safety-corresponding loop, a non-secure state is an output. The non-security state discussed herein refers to the state of the control system under the influence of the cyber incident and thus the state of an individual. Security correspondence is implemented against the output non-secure state. Safety and security's vital tenet of “connection” is the control of the global standard. With regard to safety, the OSHMS is adopted. However, with regard to security, IEC 62443 is adopted. Overall, the global standard requires a fundamental line of response from a safety perspective. As per the global standard analysis, the standard requires the PDCA cycle activities for continuous improvement. This is a practical and methodical approach for simultaneously achieving high levels of safety and security.

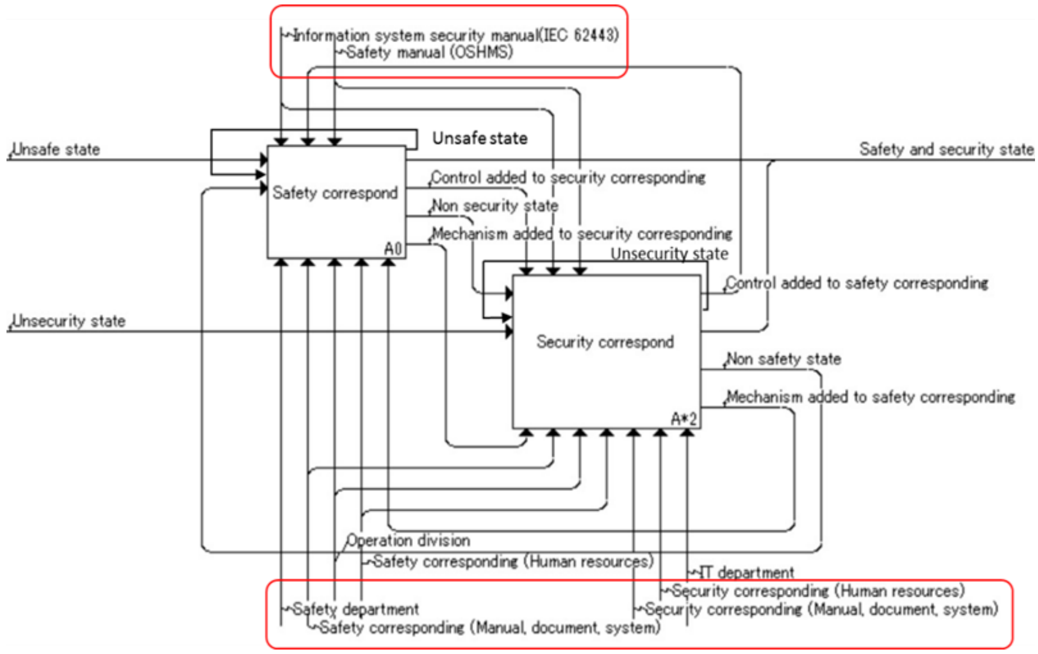


Figure 4. *Schematic of the safety and security framework*

CONCLUSIONS

In this research, a combined methodology based on IEC 62443 and OSHMS was proposed. Discussions regarding this methodology were provided based on the global standard for combining the safety and security operations to maximize resilience levels against a cyberattack that cannot be perfectly eliminated.

Future perspectives with regard to the safety and security requirements within this domain need continuous education/training of the PDCA cycle. Moreover, personnel training regimens should be adopted based on this framework. Factory operators and IT administrators need to be approached and ultimately evaluated together as a single cohort. In addition, an illustrative example of such a proposed framework and methodology was presented based on exercises wherein nearly 200 CI personnel and security experts had participated.

Acknowledgements

This research is partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (A), No. 16H01837 (2016).

REFERENCES

National Institute of Standards and Technology. (1993). Announcing the Standard for Integration Definition for Function Modeling (IDEF0). National Institute of Standards and Technology, NIST.

OHSAS Project Group. (2007). OHSAS18001: Occupational Health and Safety Management Systems - Requirement. Occupational Health and Safety Assessment Series. pp.90-179.

IEC Central Office. (2010). Industrial Communication Network-Network and system security- Part 2-1: Establishing and Industrial Automation and Control System Security Program. pp.18.

Nyambayar Davaadorj, Ichiro Koshijima, Hajime Eguchi. (2016). A Metric for Quantitative Estimation of Production Unit Based on OSHMS. 29th Symposium of Malaysian Chemical Engineers. pp.37.

Rasmussen J, senior member, IEEE. (1983). Skills, Rules, Knowledge. Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics. pp.257-266.

CRITICAL INFRASTRUCTURE RESILIENCE: BRIDGING THE GAP BETWEEN MEASURING AND GOVERNANCE

Hanneke Duijnhoven [1], Albert Nieuwenhuijs [2], Puck van den Brink [3], Dirk Stolk [4] and Theo van Ruijven [5]

[1] TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
hanneke.duijnhoven@tno.nl, +31(0)88662929
[2] TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
albert.nieuwenhuijs@tno.nl
[3] TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
puck.vandenbrink@tno.nl
[4] TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
dirk.stolk@tno.nl
[5] TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
theo.vanruijven@tno.nl

Abstract

In this paper we seek to explore the challenges regarding governance of critical infrastructure resilience by reviewing the current application of the resilience concept in the domain of critical infrastructure. We broadly discuss the most common categories of approaches towards resilience assessment of critical infrastructure resilience that are currently adopted: performance-based and attribute-based approaches. We then address differences in conceptualization andoperationalization of (critical infrastructure) resilience and discuss the implications of these different approaches with regard to their scientific underpinnings and their practical applicability for the field of critical infrastructure governance. This discussion highlights important limitations of these approaches, leading us to argue that a Resilience Engineering perspective may address some of the shortcomings of the performance-based and attribute based approaches. At the same time, the Resilience Engineering work as it stands also has some important limitations (lack of empirical evidence and practical application, as well as insufficient attention for resilience challenges within a multilevel, multi-stakeholder, network-of-networks context.

1. GOVERNANCE OF CRITICAL INFRASTRUCTURE RESILIENCE

There are many definitions of critical infrastructure and the assessment of what the critical infrastructure for a specific society consist of varies between countries. Nevertheless, in general, critical infrastructures are seen as those products, services and underlying processes that, should they fail, have the potential of causing serious societal disruptions, for instance by causing a large number of casualties, extensive economic damages or because there are no realistic alternatives available for products or services that are essential for the continuity of normal societal functions. What makes these infrastructures even more critical is that, together, they form a complex network of processes that are highly interconnected. Failures in one part of the network can cause problems in other parts of the network, potentially causing cascading impact across society that is difficult to predict.

The last decades have witnessed a widespread attention to critical infrastructure protection (and more recently resilience) across nations worldwide. Policies and legislation has emerged in many countries, as well as in the European Union, aimed at cross-border cooperation (Alcaraz & Zeadally, 2015; Klaver et al., 2008; Luiijf, Nieuwenhuijs, Klaver, van Eeten, & Cruz, 2008). In the Netherlands, the first criticality assessment to determine the critical infrastructure for Dutch society took place in 2002. Since then there have been several updates, but all following the same initial structure. In 2014 a new approach for the criticality assessment has been introduced, resulting in a new list of critical infrastructures. Whereas previously the critical infrastructures were listed in sectors and related products and services, the new approach identifies critical processes that deliver those products and services (Hamelink & Mutsaers, 2015). The assessment has been done using a range of different criteria related to the impact (physical, economic, social) of failure on society and the extent to which other processes are critically dependent on a particular process (Schoof, 2015).

As a result of the reassessment a list of processes is defined that constitute the critical infrastructure in The Netherlands. The list distinguishes between two categories of criticality (category A and category B), which has policy implications for the public and private organizations that are involved in operating and maintaining these processes. Moreover, with the reassessment, the orientation for policy is expanding from protecting critical infrastructure towards increasing the resilience of critical infrastructure (Hamelink & Mutsaers, 2015). Given the nature of the domain, with a large number of actors involved and complex networks of dependencies, increasing resilience is not something that is easily achieved. As of yet, there are no adequate governance models to address critical infrastructure resilience enhancement (Bach et al., 2013). In fact, one of the main challenges for the governance of critical infrastructures is the large, varied network of public and private stakeholders involved in combination with the connectivity, complexity and dependencies within the network of infrastructure systems.

1.1. Aim and Outline of the Paper

Given this background, this paper explores the current state-of-the-art of resilience approaches in the critical infrastructure domain in order to specify the gaps that remain. We do not intend to do a meta-analysis of resilience approaches, since there are abundant efforts in that direction. After briefly discussing the shift from CI protection to CI resilience, we will broadly discuss the most common categories of approaches towards resilience assessment of critical infrastructure resilience that are currently adopted: performance-based and attribute-based approaches. We then address differences in conceptualization and operationalization of (critical infrastructure) resilience and discuss the implications of these different approaches with regard to their scientific underpinnings and their practical applicability for the field of critical infrastructure governance. Following this analysis, we argue that a Resilience Engineering perspective may address some of the shortcomings of the performance-based and attribute based approaches, although there are still some important gaps or challenges in adopting such a perspective.

2. THE TRANSITION TOWARDS RESILIENCE IN THE FIELD OF CRITICAL INFRASTRUCTURE

The field of Critical Infrastructure research has traditionally focused on the protection and reliability of infrastructure systems in light of different causes of disturbances (threats). Recently, a shift can be observed from a focus on the protection of critical infrastructures towards a focus on critical infrastructure resilience (Alsubaie, Alutaibi, & Martí, 2015). Risk management has been a dominant orientation and is used to identify potential sources of disturbances, the potential impact of these disturbances and ways to prevent or minimize negative consequences. The increasing complexity of infrastructure systems, their increasing connectivity and network dependencies (partly due to increasing digitalization) make it impractical and perhaps even impossible to assess all risks and take protective measures accordingly (Vugrin, 2016). In addition to this, the threat landscape is also changing, with fast-moving developments such as cyber threats, geopolitical developments and technological innovation, making it ever more difficult to continue with traditional risk management approaches. Thus, it is increasingly recognized that we live in an age of uncertainty and unexpected events will always occur, so it makes sense to focus on being able to deal with unexpected situations rather than trying to prepare for every possible situation (Weick & Sutcliffe, 2007). Hollnagel argues that instead of focusing on all possible things that can go wrong it is important to focus on understanding and increasing “the ability to succeed under varying conditions, so that the number of intended and acceptable outcomes (in other words, everyday activities) is as high as possible”(2013: 8). Resilience has been widely embraced as a promising concept that embodies this shift in orientation (Duijnhoven and Neef 2014; Woods and Hollnagel 2006).

The shift towards resilience thinking is seen across a wide variety of disciplines, with many different conceptualizations and applications of ‘resilience thinking’ as a result. Originating from the field of systems ecology, the wide adoption of resilience is mostly attributed to the work of Holling (1973). From there, the concept, as a “science of complex adaptive systems and an operational strategy of risk management” (Walker & Cooper, 2011: 143) has gained traction in fields such as safety management, disaster management, systems engineering, and natural resource management (Van Ruijven, 2016). Application extends to domains such as climate resilience (resilience of ecological systems against climate change), community resilience (resilience of communities against a wide range of crises), organizational resilience (business continuity in the face of internal and external pressures), cyber resilience (resilience of {digital} systems against cyber threats), and critical infrastructure resilience (resilience of critical infrastructures against disturbances). Between (or even within) all these different approaches, there is no consensus with regard to the definition and 3 operationalization of resilience. In fact, as Woods (2015) argues, in many studies it is unclearly stated how the concept is used and why. This is problematic as it may stall progress in the field.

3. Current Approaches towards Critical Infrastructure Resilience

Definitions of critical infrastructure resilience vary and are usually inspired by the use of the term resilience in other disciplines (Alsubaie et al., 2015; Bach, Bouchon, Fekete, Birkmann, & Serre, 2013). An often cited definition in the field is that from the US National Infrastructure Advisory Council (NIAC): “the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends on its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" (2009). Definitions aside, the actual conceptualization of resilience is generally related to the reliability and robustness of the system.

When it comes to resilience analysis, several distinguishing approaches can be identified across the domain of critical infrastructures. Following the classification of resilience assessment approaches in structural, performance-based and hybrid approaches (Biringer et al. (2013) in Alsubaie et al., 2015: 45), Alsubaie et al. present a literature review of 19 approaches towards CI resilience. The majority of approaches (12) can be classified as performance-based approaches. These attempt to "evaluate the system resilience by measuring its performance before and after a disruption" (Alsubaie et al., 2015: 45). Four approaches are classified as structural approaches, meaning that they "use the structure or topology of the system to evaluate its resilience" (Alsubaie et al., 2015: 45). Three approaches are classified as 'hybrid', using a combination of structural and performance-based assessment.

Similarly, Vugrin (2016) distinguishes between two broad categories of instruments for critical infrastructure resilience assessment. At one end of the spectrum there is a group of approaches that aim to identify properties or characteristics of a system that contribute to its resilience. There is no widely accepted list of resilience attributes, but they often include attributes such as robustness, redundancy, resourcefulness, adaptability. These attribute-based approaches usually involve a qualitative (or semi-quantitative) assessment of the degree to which the system demonstrates such attributes. According to Vugrin, the benefit of this type of approach is that it is less time- or resource intensive. These approaches, however cannot really predict how resilient the system will be for future (unknown) disruptions and rely heavily on qualitative, subjective assessments. Often, these approaches have a practical orientation and are meant to be used by infrastructure operators and governmental agents to assess the resilience of the systems under their responsibility. Examples are the critical infrastructure resilience index as developed by Argonne National Laboratory (Fisher et al., 2010), approaches developed in European Horizon 2020 projects such as RESILENS 1 and IMPROVER 2 , or the approach developed by the Australian government 3 to support organizations (including critical infrastructure operators) in assessing their own resilience. The conceptualization of resilience underlying these approaches is often not explicitly stated or theoretically elaborated. At the other end of the spectrum there are performance-based approaches that aim to quantitatively measure the degree of resilience of a system by measuring the performance level of the system in case of a specified disruption (Vugrin, 2016). Often, resilience is then presented as a "time dependent ratio of recovery over loss" (Barker, Ramirez-Marquez, & Rocco, 2013). According to Vugrin, a benefit of such approaches is that they are more useful for comparative analyses (bench-marks) because they rely less on qualitative, subjective assessment. Limitations are that such approaches usually require a vast amount of data and complex (computational) modelling which is generally more time- and resource intensive. In addition, the outcome of this type of resilience assessment does not offer much explanatory information about why the system is more or less resilient. The complex models require a lot of knowledge about a system, but the actual calculation of resilience is a black box that does not contribute to a better understanding of resilience. This type of approaches has a strong scientific orientation and therefore it seems to be the dominant approach in the scientific literature on critical infrastructure resilience. The scientific orientation and high requirements in terms of data and expertise generally makes these approaches less suitable for practical application in an operational context. Often-cited examples are those by Henry and Ramirez-Marquez (2012), Barker et al. (2013), Filippini and Silva (2014), Francis and Bekera (2014), and Ouyang et al. (2014; 2012; 2015). Both ends of the spectrum offer benefits and limitations, and it is tempting to combine the strengths into hybrid approaches. However, when taking a closer look at the existing approaches, it becomes clear that many of them are not fully embracing all the concept of resilience has to offer. We argue that the critical infrastructure field could benefit from some of the progress that has been made within the Resilience Engineering field, in particular with regard to the conceptualization of resilience. In the next section we will briefly introduce the Resilience Engineering perspective and argue why this would be a useful lens in the field of critical infrastructures.

1 http://resilens.eu/resilens-outputs/

2 http://improverproject.eu/category/results/

3 http://www.organisationalresilience.gov.au/HealthCheck/Pages/default

4. ADOPTING A RESILIENCE ENGINEERING PERSPECTIVE

A resilience perspective focuses on how a system performs its/several functions and in what ways it can resist, absorb, respond, or adapt to disturbances. As such it is a fundamentally different mindset than what is common in traditional risk management methods, and it requires different methodological approaches (Vugrin, 2016). Whereas risk assessment has an external orientation, focusing on a set of specific threats that a system may be exposed to, resilience analysis focuses on the dynamic, internal mechanisms that make a system operate and contribute to stable delivery of its products or services. As such, it moves away from anticipation towards “more inclusive strategies that integrate both resistance (prevent, protect) and resilience (respond, recover)” (Longstaff, Armstrong, Perrin, May, & Parker, 2010). When it comes to resilience analysis, there are many different approaches, with different underlying conceptualizations of what resilience of complex (socio-technical) systems is and how it can be analyzed (Nemeth & Herrera, 2015). Woods (2015), recognizes four basic conceptualizations of resilience that are applied to complex adaptive systems:

1. resilience as the ability to rebound from trauma and return to equilibrium;
2. resilience as a synonym for robustness;
3. resilience as the opposite of brittleness, i.e., as graceful extensibility when surprise challenges boundaries;
4. resilience as network architectures that can sustain the ability to adapt to future surprises as conditions evolve.

These four conceptualizations are a testament to the evolution of resilience thinking as the field progresses. The first and second conceptualizations stem from earlier stages of resilience research, although they still prevail in many studies. These two interpretation are rather limited and do not fully embrace the essential notions of the resilience concept as offering an alternative perspective to address the complex, non-linear, stochastic nature of technological systems (Hollnagel, 2006; Woods, 2015). The third and fourth conceptualizations show the advances in resilience thinking and introduce new concepts such as ‘brittleness’ and ‘sustained adaptability’ into the perspective (Woods, 2015). The third conceptualization is where, according to Woods, the state of the art of resilience engineering currently stands. This perspective focuses on “how a system extends performance, or brings extra adaptive capacity to bear, when surprise events challenge its boundaries”(Woods, 2015: 5). The fourth conceptualization is where the field should be progressing towards (Woods, 2015). This conceptualization aims to identify what architectural properties contribute to the capacity of systems to continue adapting to surprises under dynamic and evolving conditions. This means that we need to understand more about what resilience looks like in practice, or more specifically it is necessary to observe empirical instances of adaptability in operational contexts (Nemeth & Herrera, 2015; Woods, 2015). An additional question, that is currently underemphasized within the Resilience Engineering community, would be how to operationalize this conceptualization in the context of dependent networks of a range of different critical infrastructures, with multiple stakeholders and often different or even competing interests. These systems tend to have a long history and many of its properties and characteristics have developed and emerged over a long time (for instance due to technological progress and processes urbanization). The notion of architectural properties seems relevant, but suggests the possibility to deliberately ‘design’ (engineer) systems. The question is to what extend this is possible in existing infrastructures, and if so, who the designer/engineer is (who can decide)?

In terms of these four conceptualizations that Woods (2015) distinguishes, most of the performance-based approaches and attribute-based approaches that are currently being developed in the field of critical infrastructure resilience seem to come close to the second conceptualization, although often this is not clearly specified. In fact, as Bach et al. argue, (Bach et al., 2013) it seems that the use of the concept of resilience in the field of critical infrastructures is not very well developed yet and the field could benefit from adopting insights from other fields that are further developed in resilience thinking. Precisely because of the criticality of 5 critical infrastructures for society, it is important to come up with effective resilience assessment approaches that utilize the multidisciplinary scientific knowledge for practical, operational applications. The third and fourth conceptualization that Woods describes may provide a good starting point, although it is necessary to further develop these idea to also address the specific challenges of a multi-stakeholder, multi-level, network of networks context such as the field of critical infrastructures.

5. CONCLUSION

The dominant approaches to resilience (as discussed in previous sections) have a rather narrow interpretation of resilience, for instance as the ratio of loss and recovery in the face of a disturbance. The performance-based approaches do not provide pointers for governance of resilience. Other approaches provide lists of attributes of resilience that can give direction as to what type of capacities a system should strive for, but these are rather subjective and do not guarantee that it constitutes sustainable capacity in changing circumstances.

What is more, most of these approaches are targeting single organizations or infrastructure systems, while from a governance perspective it is relevant to address resilience at the level of the network or even at the societal level. The conceptualizations of resilience as developed within the Resilience Engineering community offer part of the solution since it is concerned with opening up the ‘black-box’ of complex systems and understanding where its boundaries are and what the adaptive capacity constitutes (providing concrete insights to decision-makers about how to enhance resilience). It specifically aims to gain an understanding of how to achieve sustained adaptability, yet, until now there are few studies that provide empirical evidence of these conceptualizations. What is more, the literature in the Resilience Engineering community tends to focus on relatively closed systems and it does not explicitly address resilience of networks of systems at a society or intersectoral level. For the challenges in the field of critical infrastructure resilience, a successful approach should address the mutual dependencies and connections between different critical infrastructures. "Rather than focusing on the protection of certain facilities, the safeguarding of the provision of services should be the primary aim" (Bach et al., 2013). This, defining critical processes rather than critical infrastructures, as recently introduced in Dutch policy context, may offer a better starting point to assess the performance and strength of resilience attributes at the level of network-of-networks. But in order to understand how to build more sustainable resilience into these systems requires an approach that explicitly addresses this type of complex context.

REFERENCES

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53–66. https://doi.org/http://dx.doi.org/10.1016/j.ijcip.2014.12.002

Alsubaie, A., Alutaibi, K., & Martí, J. (2015). Resilience Assessment of Interdependent Critical Infrastructure. In International Conference on Critical Information Infrastructures Security (pp. 43–55). Springer.

Bach, C., Bouchon, S., Fekete, A., Birkmann, J., & Serre, D. (2013). Adding value to critical infrastructure research and disaster risk management: the resilience concept. SAPI EN.S.Surveys and Perspectives Integrating Environment and Society, (6.1).

Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. Reliability Engineering & System Safety, 117, 89–97. https://doi.org/http://dx.doi.org/10.1016/j.ress.2013.03.012

Duijnhoven, H., & Neef, M. (2014). Framing Resilience. From a Model-based Approach to a Management Process. Procedia Economics and Finance, 18(September), 425–430. https://doi.org/10.1016/S2212-5671(14)00959-9

Filippini, R., & Silva, A. (2014). A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. Reliability Engineering & System Safety, 125, 82–91.

Fisher, R. E., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., … Lawlor, M. A. (2010). Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering & System Safety, 121, 90–103. https://doi.org/http://dx.doi.org/10.1016/j.ress.2013.07.004

Hamelink, S., & Mutsaers, J. (2015). Critical Infrastructure Protection: From Protection to Resilience. European CIIP Newsletter, 9(3), 21–23.

Henry, D., & Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. Reliability Engineering & System Safety, 99, 114–122. https://doi.org/http://dx.doi.org/10.1016/j.ress.2011.09.002

Holling, C. S. (1973). Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 1–23.

Hollnagel, E. (2006). Resilience - the Challenge of the Unstable. In E. Hollnagel, D. Woods, & N. Leveson (Eds.) (pp. 9–17). Aldershot: Ashgate.

Hollnagel, E. (2013). A tale of two safeties. Nuclear Safety and Simulation, 4(1), 1–9.

Klaver, M. H. A., Luiijf, H. A. M., Nieuwenhuijs, A. H., Cavenne, F., Ulisse, A., & Bridegeman, G. (2008). European risk assessment methodology for critical infrastructures. In Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), 2008 First International Conference on (pp. 1–5). IEEE.

Longstaff, P. H., Armstrong, N. J., Perrin, K., May, W., & Parker, M. A. H. (2010). Building Resilient Communities: A Preliminary Framework for Assessment. HOMELAND SECURITY AFFAIRS, 6(3).

Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., & Cruz, E. (2008). Empirical findings on critical infrastructure dependencies in Europe. In International Workshop on Critical Information Infrastructures Security (pp. 302–310). Springer.

National Infrastructure Advisory Council. (2009). Critical Infrastructure Resilience: Final Report and Recommendations. US: National Infrastructure Advisory Council.

Nemeth, C. P., & Herrera, I. (2015). Building change: Resilience Engineering after ten years. Reliability Engineering & System Safety, 141, 1–4. https://doi.org/http://dx.doi.org/10.1016/j.ress.2015.04.006

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety, 121, 43–60. https://doi.org/http://dx.doi.org/10.1016/j.ress.2013.06.040

Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. Structural Safety, 36–37, 23–31. https://doi.org/http://dx.doi.org/10.1016/j.strusafe.2011.12.004

Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. Reliability Engineering & System Safety, 141, 74–82. https://doi.org/http://dx.doi.org/10.1016/j.ress.2015.03.011

Schoof, D. (2015). Wat is vitaal? Magazine Nationale Veiligheid En Crisisbeheersing.

Van Ruijven, T. (2016). Multidisciplinary Emergency Management. A comparative study of coordination and performance of on-scene command teams in virtual reality exercises. Delft: Delft University of Technology.

Vugrin, E. D. (2016). Critical Infrastructure Resilience. In IRGC (Ed.) (v. 29-07-20). Lausanne: EPFL International Risk Governance Center.

Weick, K., & Sutcliffe, K. (2007). Managing the unexpected: resilient performance in an age of uncertainty. John Wiley & Sons, Inc.

Woods, D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 141, 5–9. https://doi.org/http://dx.doi.org/10.1016/j.ress.2015.03.018

Woods, D., & Hollnagel, E. (2006). Prologue: Resilience Engineering Concepts. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.) (pp. 1–16). Aldershot, UK: Ashgate Publishing Limited.

A PRACTICAL WORKSHOP-BASED METHOD TOWARDS RESILIENT DESIGN OF COMPLEX SOCIO-TECHNICAL SYSTEMS

M.H.C. Everdij [1] and S.H. Stroeve [2]

[1,2] Netherlands Aerospace Centre, Amsterdam, The Netherlands

[1] everdij@nlr.nl, [2] stroeve@nlr.nl

http://www.nlr.org

Abstract

Under the premise that a more resilient operation is better able to be safe and efficient, this paper presents a pragmatic approach for analysing the resilience of future air traffic management (ATM) operational concepts and improving their design. The approach uses a workshop with operational experts as a central element and follows 5 steps. The last two steps use key new elements specific for this approach; the first three steps are used in other safety methods as well, but are adapted to better support the last two steps. The approach is illustrated through application to an ATM operational concept that uses an Aircraft Surveillance Applications System (ASAS) for sequencing and merging of aircraft towards an airport. The output is an analysis of the resilience of the operation, and the identification of a range of recommendations for the design of this operation, such that its resilience can be improved.

1 INTRODUCTION

Before a design of an air traffic management (ATM) system can be put into operation, an analysis needs to show that it is sufficiently safe. Most of the focus of today's safety management systems is put on the identification and mitigation of hazards and failures. However, failure situations are rare and hence present a very limited picture when trying to design a socio-technical system that is safe as a whole. In the perspective of Safety-II and Resilience Engineering (RE) (Hollnagel, 2014), successes and failures of the socio-technical system both stem from performance variability. Different varying conditions may combine to hazardous situations due to their complexity and intractability. Not all such conditions can be expected and prepared for beforehand, and unexpected conditions will at some point occur. RE defines safety as the ability to succeed under both expected and unexpected varying conditions. Moreover, RE emphasises the need to well consider the multiple goals that the socio-technical system aims to achieve, which is not only safety but often also productivity, security, environmental sustainability, etc.

For an RE approach to be successful it will need to include: 1) a way to analyse the resilience of an operational design; and 2) a way to improve the operational design in order to make it more resilient. Without the first element, there is no way to understand where resilience comes from and where it can be improved. Without the second element there would be no engineering of resilience back into the design. The proper execution of these two elements requires experts in resilience and safety analysis, and operational experts. For ATM designs, the operational experts include air traffic controllers, pilots, supervisors, technical engineers, maintenance engineers, etc. These operational experts can change gears quickly and are trained in dynamically and creatively handling various new occurrences. They have the ability to deal with varying conditions and interacting human operators and technical systems in an operational context, and they have the ability to imagine themselves in a new context, such as a future operational design. As such, they have knowledge and experience that is essential not only for element 2 above (improving the operation), but also for element 1 (resilience analysis).

The RE approach presented in this paper makes effective use of operational experts in both the resilience analysis and the improvement of the operation, but uses limited RE jargon. A central element in the approach is the identification of the strategies that the operational experts use when dealing with varying conditions (or combinations thereof) in their daily work. The result of the RE approach is a deeper understanding of how the socio-technical ATM system deals with small and large, common and rare disruptions and conditions, at a level sufficient to identify improvements to the operational design.

This paper presents the results of application of the RE approach to a specific operational concept of Aircraft Surveillance Applications System Sequencing and Merging (ASAS S&M) conducted in (Everdij et al., 2016). The approach followed took as input the lessons learned during earlier applications of RE, such as (Herrera et al., 2015). The objective of the current study was to test and further improve the RE approach by its application to the ASAS S&M concept in the design phase. It should be noted that the ASAS S&M concept is under development and that this paper does not conclusively evaluate the ASAS S&M concept. The paper merely aims to illustrate the RE approach, by using the ASAS S&M concept as a case.

The paper is structured as follows: Section 2 describes the RE approach, Section 3 describes the application to the case of ASAS S&M and presents some of the key results, Section 4 provides a discussion.

2 RE APPROACH

The RE approach has 5 steps, which follow Figure 1 below. The activities include (but are not limited to) the four main sessions of an RE workshop with participation of operational experts.

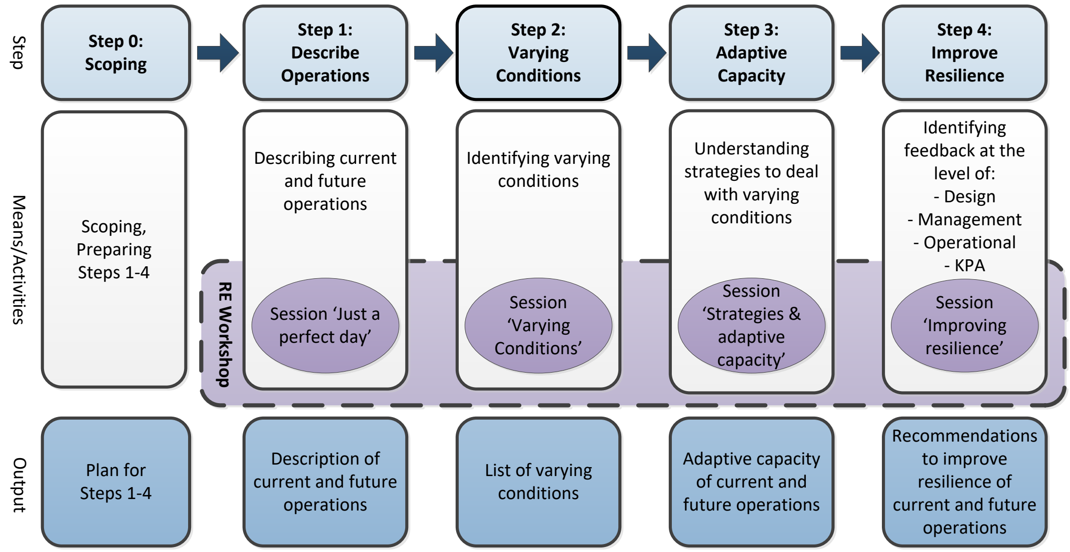


Figure 1. *The RE approach follows five main steps*

The *Scoping* step (step 0) aims to plan and outline the study. The activities include developing the RE workshop structure and agenda, and arranging the logistics. The *Describe Operations* step (step 1) aims to build an initial understanding of the work-as-done in current ATM operations and of the way that future ATM operations are expected to be done. The activities include studying relevant material, interviewing experts, and doing observations in the field and at simulation facilities if feasible. The *Varying Conditions* step (step 2) aims at identifying a list of varying conditions that ATM operators and managers may have to deal with in the future and current ATM operation. The activities include studying relevant material such as safety analysis documents on related operations, and organising brainstorm sessions with operational experts. The *Adaptive Capacity* step (step 3) aims to obtain narrative descriptions of the strategies that operators and supervisors use when they are dealing with varying conditions in the current and the future ATM operation, and to analyse the adaptive capacity of the current and the future ATM operations. The activities include organising workshop sessions with air traffic controllers, pilots, and supervisors, as well as applying appropriate techniques to determine the adaptive capacity these operational experts have when dealing with varying conditions. The *Improve Resilience* step (step 4) aims at deriving recommendations for strengthening the resilience of current and future ATM operations. These recommendations are aimed to be translated into new or revised design requirements. The activities include a brainstorm session with the operational experts involved in step 3, who are asked to identify design improvements at the levels of design, management, operation and key performance areas such as safety, capacity, environment and cost-benefit. In addition, complementary design improvements are identified through analysis of all material collected so far.

3 APPLICATION

The RE approach was applied to a specific future operational concept of ASAS S&M, set around a large European airport. The pilots on flights enabled with ASAS S&M can get an instruction from the air traffic controller to maintain a certain spacing (a time distance) with a specific target aircraft in front of them. This target aircraft can be on the same route ('sequencing'), or on another route that merges with the route of the follower aircraft ('merging'). This operation differs from current operations, in which aircraft get heading (directions) and speed instructions from the controller to safely sequence and merge on their routes.

The ASAS S&M operation was set in the context of a larger operation, with an extended arrival management system supporting controlled time of arrival operations on an extended operational horizon. The airspace for the larger operation consisted of 6 sectors, but during the RE workshop, the main focus was on the sectors nearest the airport, where ASAS S&M was used. These were two terminal manoeuvring area (TMA) sectors and one arrival (ARR) sector. In addition there was the final approach sector (TWR) which included the runway itself. For each sector there was one executive controller. There was one supervisor for the TMA/ARR sectors, and one supervisor for TWR.

3.1 Step 0: Scoping

As part of step 0, a plan was developed for the activities to be conducted in steps 1-4, including RE workshop structure and agenda, the physical and electronic material to be used, and logistics like list of participants, meeting room venue, and role of each RE team member. Figure 1 shows the main sessions planned for the RE workshop. These were preceded by an introductory session to explain the purpose of the workshop and to summarise the ASAS S&M design. A debriefing was prepared in which the participants were to be asked for their feedback on the workshop organisation. One of the main concerns in the planning was to make sure that the activities had the appropriate set of well-experienced participants. For the RE workshop, we were able to invite 5 controllers with experience of the relevant air traffic control positions and including a supervisor, and 2 experienced airline pilots. In addition, there were between 2 and 6 observing participants with various ASAS and/or safety expertise. The RE team consisted of 5 members; two for moderating the workshop and making notes; one for leading the step 4 session; one in charge of the logistics, and one in charge of the debriefing.

3.2 Step 1: Describe operations

As part of step 1, the RE team studied available documentation on current and future ATM operations, including operational service and environment descriptions (OSED), validation plans, procedure and rule sets, etc. In addition, the team made observations during large-scale human-in-the-loop simulation sessions of the ASAS S&M operation. These human-in-the-loop simulations used experienced planning and executive air traffic controllers for each of the controller positions, who were tasked to safely and efficiently control traffic flown by over a dozen pseudo-pilots and one cockpit simulation. The simulations took place during two weeks plus one week of training, and were organised by a project in charge of validating the ASAS S&M concept in a larger context. During a few days, the RE team attended these simulations as guests in order to observe how the operators (i.e. controllers, pilots, supervisors) act and interact with each other and with their human machine interface and environment. An additional means used in step 1 was Session "Just a perfect day" in the RE workshop (see Figure 1). Herein, the participating operational experts (controllers, pilots, supervisors) explained what a typical day of operations without considerable varying conditions ('just a perfect day') looks like for them in their current work. Next they were asked to express their expectations of what such a perfect day would look like in the future ASAS S&M operation. This session served to achieve a common understanding of the operations from various perspectives. It is noted that the operational experts involved in the RE workshop were also part of the human-in-the-loop simulations described above. This significantly helped them in their operational comprehension of this future operation.

The information obtained from these means was summarised and documented, with references to the source of the information. The output was a better understanding of the ASAS S&M operation, the dynamics involved, the timing of activities, the human-machine interface, human-machine interactions, and the controller-controller and controller-pilot communications.

3.3 Step 2: Varying conditions

The main source for step 2 was a dedicated brainstorm session, organised with ATM operational experts as part of the RE workshop (see Figure 1). The operational experts were each given several prepared forms, and were asked to write down as many conditions as possible; rare conditions as well as normal conditions, and to consider situations within their control as well as situations outside of their control. During the brainstorm, a total of 49 varying conditions were identified, which (after the workshop) were organised into 12 clusters of similar or related conditions, i.e. Adverse weather conditions, Runways & taxiways conditions / availability, Airspace restrictions, Separation issue / missed approach, Traffic load evaluation, Differences in aircraft performance, Flights with emergency conditions, Controller performance, Pilot performance, Air Traffic Control system problem, ASAS S&M system unable to find solution, and Aircraft system problem. The list included conditions that could be considered hazards, or situations with the potential to compromise safety, but there were also several 'normal' situations, such as temporary airspace restrictions, cultural differences, or situations with mixed traffic, such as arrivals of medium and heavy weight aircraft on a single runway, which controllers and pilots have to deal with in their daily work.

3.4 Step 3: Adaptive capacity

This step included two distinct sub-activities. The first included the organisation of Session "Strategies & Adaptive Capacity" in the RE workshop (see Figure 1). In this session, for each cluster of varying conditions identified in step 2, a representative varying condition (or a combination of such conditions) was selected and the operational experts (controllers, pilots, supervisors) were asked to explain the strategy or strategies they use or envisage to use when dealing with this varying condition; first in current operations, and next in future ASAS S&M operations. Each such strategy description was derived by asking appropriate questions; Table 1 presents the question set used for this. This set was designed to cover the principles of resilience (see also discussion in Section 4) and it uses terminology that corresponds to the experience of operators in ATM. The results of the session were documented in narrative form, describing what the participants said as well as possible, thus making sure that the context in which they said it was captured. This provided the raw data that could be used as input to the more detailed adaptive capacity analysis.

Table 1. *Questions used to elicit operator strategies per varying condition. They were used for both current and future operations*

Frequency	In what way and how often could the varying condition occur?
Detection	Who or what would detect the varying condition, and how?
Strategy / Adaptation	What is the strategy to deal with the varying condition, i.e.: How would you act / adapt to the varying condition, with whom would you interact and coordinate, what resources are used?
Learning / Training	How is the strategy acquired, for instance is it part of basic training, is it learned by experience?
Trade-offs	What are the trade-offs and what are the effects of applying the strategy on ATM key performance areas such as safety, capacity, costs, and environment?

The second sub-activity, executed after the RE workshop, was to analyse 'base and extra adaptive capacity'. This technique was loosely based on the Stress-Strain model of Woods et al. (2013), which is a framework for analysis of how a system stretches to handle surprises. In the technique, for each varying condition discussed in the RE workshop, and for both the current operation and the ASAS S&M operation, the capacity of the ATM system to recognise and handle the varying condition was identified. In some situations this capacity involved the use of elements already covered by the design of the ATM system, including procedures and training (base adaptive capacity); in some situations it required more creativity and experience from the human operators (extra adaptive capacity). The notes of the RE workshop were used as the input to this analysis. For each varying condition, the results were documented using the format of Table 2. The table was next analysed in order to investigate trends between the results for the different varying conditions. For several situations and varying conditions, the strategies for dealing with them appeared to be not covered by procedures and training, but to be learned on the job. Controllers and pilots require experience and creativity when they are confronted with these situations.

Table 2. *Presentation of analysis results of the base and adaptive capacity per varying condition*

<table>
<tr><td colspan="2">Varying condition. Here the ID and brief description of the varying condition is discussed</td></tr>
<tr><td>Adaptive capacity in current operation. Description of the way that the varying condition can be recognized in the current operation, how it can be handled by the pilots and by the controllers, and the implications for the base or extra adaptive capacity.</td><td>Adaptive capacity in future operation. Description of the change in recognition, strategies, and adaptive capacity of the future ASAS S&M operation in comparison with the current operation.</td></tr>
<tr><td>Summary. Summary of the above, in terms of base and extra adaptive capacity required by controllers and pilots in current operation.</td><td>Summary. Summary of the above, in terms of the change in adaptive capacity required by controllers and pilots in future operation compared to current.</td></tr>
</table>

3.5 Step 4: Improve resilience

For this step, a brainstorm session with operational experts was organised as part of the RE workshop (session "Improve resilience" in Figure 1). Herein the experts were split up into smaller groups and were asked to identify measures to improve the resilience of current and future ATM operations at four levels:

- Design level, including hardware and software, human factors, procedures, airspace structure, layout of the workplace, etc.
- Management level, including supervisors, managers and their procedures and processes for managing and controlling the organisation.
- Operational level, including training, organisational learning, team considerations, safety culture, etc.
- KPA (Key Performance Areas) level, including effects on safety, capacity, environment, cost-benefit.

It was key to have this brainstorm session near the end of the RE workshop, such that the earlier sessions created an environment of thinking in terms of resilience and adaptive capacity. After the RE workshop, the documented results of steps 1, 2 and 3 were reviewed and analysed by the RE team in order to identify additional improvements and making sure that nothing was missed. Subsequently, the improvements identified through the above means were formulated by the RE team as recommendations to improve the resilience of future ATM operations, which were next reviewed by operation designers.

For the ASAS S&M case, the identified improvements included requirements to re-design the airspace and adjacent sectors in order to better accommodate the new operation. Also, a need was identified for a new tool to assist the controller in converting spacing distance to seconds, and that displays the spacing time between aircraft. There was also a need to set a maximum to the traffic capacity in ASAS S&M operations, at a level that can be effectively downsized in the case of sudden runway capacity reduction. The pilots identified a need to get information during their pre-flight briefing on whether the ASAS S&M procedure is in use at the destination airport, because this would have impact on the amount of fuel to take.

4 DISCUSSION

This paper presented a pragmatic approach for RE. The workshop-centred RE steps were successfully applied to the current and to ASAS S&M approach operations. This led to the identification of a range of recommendations for the design of the future ASAS S&M operation, such that its resilience can be improved.

Steps 0, 1 and 2 are preparatory, and have similarities with many other safety analysis methods. Nevertheless, their proper execution is essential to the success of the application. Especially in step 2 (varying conditions) it is important to maintain a wide scope, and include not only hazardous situations but also situations that are considered part of the daily job, and that call for the operator’s attention because they require coordination and communication.

Steps 3 and 4 are specific for this RE approach, even though some elements are also used elsewhere. The first subactivity of step 3 (identification of strategies) has been designed to address all principles and aspects of resilience such as those defined in (Woltjer et al., 2015). E.g., ‘signals and cues’ is addressed by the question how the condition can be detected, and how it is monitored while it unfolds; ‘margins, adaptive capacity’ is addressed by the question that asks about the strategy when dealing with the condition; ‘timing and synchronisation’ and ‘cascading’ are addressed by the questions that ask how the experts interact and coordinate while the situation unfolds; ‘under-specification’ is addressed by the question about training or experience; ‘goal trade-offs’ is addressed by the question that asks about the trade-offs; ‘work-as-done’ and ‘varying conditions’, are addressed by asking the experts about their strategy when dealing with a varying condition, and by sessions ‘just a perfect day’ and ‘identification of varying conditions’ in the workshop.

The second subactivity of step 3 (analysis of adaptive capacity) uses this as input to analysing the resilience of the ATM socio-technical system, by way of analysing how this socio-technical system adapts to varying conditions. This paper illustrated the use of a technique called base and extra adaptive capacity analysis, which distinguishes situations that are covered by procedures and training (base adaptive capacity), and situations that require experience and creativity from the operators (extra adaptive capacity). The focus is primarily on individuals, either at the sharp end or at higher managerial levels, and on how they interact with other individuals, technical systems and their environment. More advanced techniques are required to get to a level of resilience emerging out of multiple complex and dynamic interactions between multiple operators and their environment. Stroeve & Everdij (2017) discuss what it takes to be able to address such challenging levels, and show how agent-based modelling and simulation can be effectively used to this end. The agents in such model have time-dependent states, inputs and outputs, and the evolution of these states, the impact of the input signals on the states, and the implications of the states for the output signals are represented by sets of model constructs. These model constructs include key constructs for the agent’s situation awareness in a multi-agent environment, task-related (identification, scheduling, execution, decision making) model constructs, task load and contextual control mode as workload-related model constructs, and variability-related model constructs representing dynamics, stochasticity and errors in human performance. Together with constructs for technical systems performance and environment, they form a model that is effectively used for qualitative or quantitative analysis of resilience of complex systems.

The success of step 4 is for a large part dependent on the proper execution and success of step 3. For one, the workshop moderators need to make sure that all aspects of resilience are addressed. Therefore, it is important that these moderators are trained in the principles of resilience and Safety II, and are able to subtly steer the operational participants into thinking in terms of these principles as well, without using the associated jargon. Secondly, step 3 helps the operational experts to get a mind-set of thinking in terms of resilience, rather than for example in failures and errors. Thirdly, the operational experts get a chance to talk about their daily work in a systematic way, and with other operational experts. This helps them look for areas in which their job can be improved and how their actions affect others. For this, it is important that step 3 covers a wide area of varying conditions and the strategies to deal with them. Fourthly, it is important to have an appropriate and complementary set of participants, including experienced controllers, pilots, supervisors and technical personnel. The most valuable output emerges from the interaction between these experts.

The success of step 4 also benefits from the results obtained in the other steps. The information collected in the observations of the human-in-the-loop simulations, the 'Just a perfect day' session, the 'Strategies and adaptive capacity' session, and the analysis of base and adaptive capacity or the use of more advanced techniques after the workshop each provide input to the identification of design recommendations. The analysis of the complete collection of inputs provides background material and justification for the recommendations, and makes sure that nothing relevant is missed.

The operators in our RE workshop were very positive about the approach, which allowed them to explain all the things they do to make ATM safe, rather than getting blamed for some rare and difficult situations they were not able to completely solve given the circumstances. During the debriefing, they explained that before the workshop, the term 'resilience' was just a word. But now, it appears to be a part of life, something that they use in their everyday work.

Acknowledgements

The research reported upon was funded as part of the SESAR Joint Undertaking within P16.06.01b. We gratefully acknowledge the contribution of operational experts (especially air traffic controllers, and staff association and airspace user representatives) and project members and safety experts of the ASAS S&M projects, and the SJU P16.06.01b project members from ENAV (especially Massimiliano Bottone and Marco Paino), INDRA (especially Cristina Díaz Domínguez), NORACON (especially Billy Josefsson), EUROCONTROL (especially Ella Pinska) and IFATCA (especially Tom Laursen). The views and opinions in this publication are of the authors and are not intended to represent the positions of SESAR JU or its project member organisations.

REFERENCES

Everdij, M., Stroeve, S., Bottone, M., Díaz Domínguez, C., De Gelder, N. & Paino, M. (2016). *ASAS - Interim Report 2014*, SESAR Project 16.06.01b: Application of Resilience Guidance to Multiple Remote Tower and ASAS S&M, Deliverable D03-001

Herrera, I., Smoker, A., Pinska-Chauvin, E., Feuerberg, B., Schwarz, M., Josefsson, B. (2015) Resilience engineering (RE) in design: initial application of a new RE assessment method to the multiple remote tower concept. *Proceedings 6th REA Symposium: Managing Resilience*

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Farnham, UK: Ashgate

Stroeve, S.H. & Everdij, M.H.C. (2017). Agent-based modelling and mental simulation for resilience engineering in air transport, *Safety Science*, 93: 29-49

Woltjer, R., Pinska-Chauvin, E., Laursen, T. & Josefsson, B. (2015). Towards understanding work-as-done in air traffic management safety assessment and design. *Reliab. Engineering & System Safety*, 141: 115-130

Woods, D.D., Chan, Y.J. & Wreathall, J. (2013). The Stress-Strain Model of Resilience Operationalizes the Four Cornerstones of Resilience Engineering, *Proceedings 5th REA Symposium: Managing Trade-offs*

FLEXIBLE PROCEDURES TO DEAL WITH COMPLEX UNEXPECTED EVENTS IN THE COCKPIT

Joris Field [1], Amy Rankin [2], Frederik Mohrmann[1], Edzard Boland[1] and Rogier Woltjer [2]

[1] Netherlands Aerospace Centre NLR, Amsterdam, the Netherlands

[1] joris.field@nlr.nl, frederik.mohrmann@nlr.nl, edzard.boland@nlr.nl

[2] Department of Computer & Information Science, Linköping University, Linköping, Sweden

[2] amy.rankin@liu.se, rogier.woltjer@liu.se

http://www.man4gen.eu/

Abstract

Modern airliner operations consist of an environment with multiple detailed procedures to cover critical abnormal events and with systems that are automated and highly reliable. Complex and unexpected events are rare and may thus present a challenge to the crew to deal with, putting demands on the resilience of the crew. In the EU Man4Gen project a "flexible procedure" was developed as a strategy to assist flight crew in dealing with unexpected events where an existing procedure was not available. This procedure is intended to assist crews in adapting their response to the situation and be more flexible in their application of their procedures and training to increase the effectiveness of their response. This paper describes the procedure and its development within the project based on two sets of flight simulator experiments with operational flight crew. The resulting flexible procedure consists of steps to help crews manage time criticality, manage (un)certainty and finally to plan for contingencies and changes. This forms the basis of the discussion of how procedures can be a source of resilience in the cockpit, rather than forming a barrier to it.

1. INTRODUCTION

Modern flight crew operate in an environment with multiple detailed procedures to cover critical abnormal events, and with systems that are automated, and highly reliable. In this environment, complex and unexpected events without a clear procedure or systems solution (such as a systems reset) are rare, and may therefore present a challenge to the crew in knowing how to assess the situation and decide on a course of action (Casner, Geven & Williams, 2013; Dekker et al. 2008; Klein et al. 2004). Examples of such events are the engine explosion that occurred on Qantas Flight 32, leading to a multiple systems failure (ATSB, 2011). The Qantas Flight 32 accident exemplifies how an experienced flight crew initially try to apply procedures as required, but eventually need to adapt their response to the situation that they faced and be flexible in the application of the procedures.

The research team in the EU FP7 "Manual Operations of 4th Generation Airliners" project set out to investigate the strategies used by pilots in unexpected events through interviews (Rankin, Woltjer, & Field, 2016) and a set of exploratory simulator experiments. The results of these interviews and experiments were used to develop a strategy to assist flight crew in an unexpected event, in the form of a procedure that was flexible in its application. This paper describes the development of the procedure, the philosophy behind the different phases of the procedure and how it was validated in a follow-up experiment.

The aim of the research project was to investigate the ways in which flight crew handled the multiple failures, and environmental challenges, and the potential for assisting crew in responding to unexpected situations more effectively. In the already highly proceduralised environment of the modern airliner cockpit, the addition of a procedure is a solution that should be treated with care. While procedures form a key part of the safety process in the cockpit, there is also a risk associated with applying procedures without fully understanding their purpose. Procedures are usually developed to address a particular failure or situation, and a change in the particular situation can lead to the procedure no longer being appropriate. For example, in the situation of a complex or multiple failure, it can be difficult to identify the most appropriate procedure to apply because several procedures are applicable, and the priority of the different procedures is not easy to identify – for example where an engine failure causes multiple systems to fail. In order to avoid these potential limitations of a procedure we developed a strategy that could be used by flight crew to handle unexpected and complex situations that don't have a single "good" solution, but where multiple solutions could be effective. This strategy would have the structured elements of a procedure, but would also be generic and flexible enough to be able to cope with many different situations – a flexible procedure.

2. EXPERIMENT 1: EXPLORATORY EXPERIMENT

An initial set of experiments that was carried out in theMan4Gen project with 20 crews of line pilots identified that there was a potential for an unexpected or surprising situation to develop into a serious problem if the situation is not rapidly understood. The experiment scenarios included complex unexpected events, such as a bird strike that caused problems on multiple engines. The aim of these scenarios was to create a situation with multiple conceivable options for strategies of how to cope with a problem, where there was no single correct strategy based on normal operating procedures. In some cases the flight crew could take decisions and carry out actions that did not effectively manage the risks, or even increased the risk to the aircraft and flight.

The initial experiments in Man4Gen were carried out to identify the strategies that were applied by flight crew when faced with an unexpected, complex, situation (Field et al. 2016). These experiments identified not only the successful actions and decisions, but also the problems that were observed in the way that the crews responded to the situations. Across the results from the crews, there were three main areas that were identified for potential improvement in the development of the procedure:

1) Threat assessment – crews often experienced a high level of temporal stress and therefore expedited their decisions and actions without sufficient understanding of the situation at hand.

2) Problem solving structure – by improving the structure behind problem solving, crews are assisted in checking whether the procedures and actions suggested by the aircraft systems (e.g. the Electronic Centralised Aircraft Monitor, ECAM; or Engine Indicating and Crew Alerting System, EICAS) are applicable based on the information that they have.

3) Defining goals – identifying, comprehending and defining goals and an associated progress review would assist crews in deciding on an appropriate course of action and in checking how effective their actions are in achieving the goal.

2.1. Development of procedure

All three problems are intertwined, and the aim was to develop a flexible procedure that would assist crews in addressing all three. The concept behind the flexible procedure was to develop a strategy that would assist flight crew, in a format that would be familiar to them – the procedure – while not prescribing all of the actions to carry out in detail. A key element of the flexible procedure calls on the flight crew to "consider" carrying out the steps. In this way the flexible procedure requires the flight crew to actively develop their understanding of the situation and thereby guide them in assessing and carrying out actions appropriate to the situation. The strategy and flexible procedure was developed by a team consisting of human factors experts, operational flight crew, and operational experts from the industry. It was reviewed by representatives from the project members and tested using airline flight crew.

2.2. Procedure philosophy

The procedure combines the concepts of improving crew threat assessment and assisting their ability to manage uncertainties. This failure management procedure aims to assist crews in managing surprising, unexpected and diffuse situations where conventional training and published procedures may be insufficient. The procedure philosophy encompasses three concepts:

1) Manage time criticality
2) Manage uncertainty

3) Plan for contingencies and changes

The design parameters for the procedure are that it should be concise, logical and easy to remember. The steps in the procedure should be aligned to current operating principles and training, and supplement the existing manufacturer and operator's procedures. Flight crews should also be able to relate to the logic of the procedure so that the way it is presented aligns with their training. Furthermore, the procedure should be designed to limit the cognitive load on pilots at the start of the procedure (in consideration of stress and emotional responses), but as initial stabilisation of the situation may free crew cognitive capacity, the procedure should engage this increased capacity in higher level problem solving. The procedure also includes elements that can be applied depending on the situation that the crew faces in order to focus their decisions and actions on the most appropriate course.

2.3. Procedure phases

This philosophy was translated into a flexible procedure that consisted of six phases that covered the three concepts discussed above through a series of workshops with pilots and human factors experts. Phases 1, 2 and 3 were intended to manage the time criticality; Phases 4 and 5 manage the uncertainty; Phase 6 consists of the planning for contingencies and changes:

Phase 1: Stabilize flightpath

Phase 2: Mitigate immediate threats

Phase 3: Short term planning

Phase 4: Identify situation

Phase 5: Perform appropriate actions

Phase 6: Long term planning

Each of these phases consists of a number of reminder steps and suggestions for decisions and actions that could be taken by the crew to address the situation.

Phase 1: Stabilize flight path

The first phase is aligned with the crew response to an unintended deviation of the flight path, and includes the already likely memorised steps that can be performed immediately without specific reference to the procedure. It is included to highlight the importance of controlling the aircraft and flight path, and thereby regain composure in the situation. By including it as the first step, it also emphasises that subsequent steps in the procedure should not be carried out until sufficient aircraft control has been established. The phase is concluded with the division of Pilot Flying (PF) and Pilot Monitoring (PM) tasks between the crew in order to remind the crew to consider the options that are available to them and reinforce the active problem solving role of the monitoring pilot. We emphasize the division of these tasks for two reasons: 1) it prevents two crew members diagnosing the problem at the same time and forgetting to fly, and 2) it must reinforce the active problem solving role of the PM in this situation. In other words, who is best suited for which role in this particular situation?

Phase 2: Mitigate immediate threats

After Phase 1 guides immediate aircraft recovery with regards to flight control, Phase 2 guides immediate aircraft recovery with regards to aircraft/system integrity. At this point crews take care of the second most critical aspects, after controlling the aircraft; immediate threats. Immediate threats are those which may have a severe effect on aircraft integrity and/or controllability (Both internal and external events). Put plainly, mitigating immediate threats prevents the aircraft from falling from the sky (in conjunction with flight path control).This could be, for example, addressing a serious engine fire or flight controls failure and putting the aircraft back onto a stable flight path.

Phase 3: Short term plan

After Phases 1 and 2 are completed, the crew will have information telling them whether the aircraft will be out of their control in the immediate minutes, or not. If either Phase 1 or Phase 2 leaves many control issues/immediate threats remaining, then the crews may acknowledge that they do not have time and must land as soon as possible. However, provided they have control of the aircraft and the actions in phase 2 were effective in mitigating the immediate threats, they then must acknowledge that they have time to regain a better understanding of the situation, and resolve/prepare accordingly. Based on this "criticality acknowledgement", they must define a short term plan before continuing (especially considering a split cockpit situation). A short term plan describes the flight plan for the next 5, 15 or 30 minutes depending on the time available.

Phase 4: Identify situation

In Phase 4 the crew is tasked with understanding the nature of the situation (both failures and context), before proceeding to verify it and perform appropriate actions in Phase 5.

Usually in basic, single failure cases, the failure or situation may be non-complex and the process of problem identification is concise and intuitive. However, iIn the context of complex and ambiguous situations, familiar and rapid responses may be less effective or even detrimental, and may contribute to undesirable states and a (further) lack of understanding of the situation. In these situations it is particularly important to be aware whether the situation may be different than initially assumed or expected, and in which ways. In unclear situations, this phase may assist crews with steps geared to setting up a mental model of the situation at hand, which will support Phase 5 in determining what actions and procedures are most likely to be suitable/effective/safe given the situation.

Phase 5: Perform appropriate actions

In Phase 5 the crew will perform actions to further resolve the situation or reconfigure to a more desirable state.

Usually in basic, single failure cases, published and prescribed checklists will provide crews with the resolution required. However, complex and ambiguous situations may not be as clear cut. There may be situations where several procedures/checklists can be applied, and where it is not clear what the priorities are. In such situations, certain checklists may still assist a crew in developing understanding of the situation (e.g. troubleshooting checklists), but crews must acknowledge the limitations that these procedures have when encountering such complex, ambiguous situations.

In order to maximize rebuilding of the understanding of the situation, maximize checklist suitability and efficacy and, importantly, prevent inadvertent application of unsuitable checklists or checklist items, crews must acknowledge what they intend to do or learn with this checklist, and ensure that the procedure is safe to apply. In most cases such considerations are intuitive and part of a familiar process, but in complex and ambiguous situations, it may be a simple safeguard against undesirable states and a further loss of understanding of the situation.

Phase 6: Long term planning

Phase 6 is the final phase, in which the crews plan their flight continuation after managing the failure situation. This phase is twofold: first of all crews must ascertain what the effects of the failure(s) are. Second of all, crews must determine what the most suitable continuation plan is pertaining to other flight aspects such as weather, company considerations, and approach & landing considerations.

3. EXPERIMENT 2: PROCEDURE VALIDATION

A second set of experiments was conducted in the Man4Gen project to validate the flexible procedure. Similar to the initial experiment, a complex scenario was flown in the simulator that was intended to be challenging to the experienced crew who participated. A total of 15 crews (30 participants - captain and first officer) participated in the two flight simulator experiments (18 participants on a long-haul aircraft, 6 crews on a short-haul aircraft) to evaluate the procedures. The scenario in the experiment was a flight with a lightning strike after takeoff which affected the engine computers, a minor engine warning prior to the lightning strike added to the ambiguity of the situation.

The experiment results evaluating the procedure indicate that the crews identified that the procedure tended to assist in effective time management and reducing the temporal stress of the unexpected situation. The crews found the procedure intuitive and flexible, but rated the support for contingency planning neutrally. The results indicated that the crews that took more time for their decision making made more effective assessment of the situation which leads to a better performance in their choice of route after the lightning strike. The analysis of the results of this experiment is further described in Mohrmann et al (2017).

4. DISCUSSION & CONCLUSIONS

The results of the experiment indicate that the better performing crews in the scenario benefitted from the structured approach to the assessment of the situation. The crews that applied the structured approach were able to spend more time in the latter phases of the procedure – identifying the situation, performing the appropriate actions and formulating a long-term plan -– with respect to their route management and troubleshooting of the engine problems. The initial phases of the procedure were intended to cover the initial actions that the crew carry out to stabilise the situation and determine the severity of the situation. These initial actions include the immediate actions that crews are expected to carry out to stabilise the flight path, which would include the memory items for example. Many of the crews did not spend as much time on these initial phases, or actively verbalised the procedure during these phases, which could be explained by the crew's familiarity with these initial steps and the scenario design.

In the highly proceduralised environment of the modern airliner cockpit, with well-trained crews, extensive automation and extremely reliable systems, it is interesting to explore the potential benefits that a flexible procedure concept could have on the resilience. Despite the high level of safety, the aviation industry still strives to improve and resilience to cope with unanticipated, or multi-failure situations. The strategy that is described in this paper is a way of further assisting crews in applying their training and experience in order to effectively deal with an unexpected situation. The flexible procedure offers a method to assist the crew members in detecting potential mismatches between their understanding of the situation and better be able to identify whether immediate action is needed and how much time is available for decision making. In turn, the crews would then be better able to quickly re-frame and understand the situation following an unexpected event.

Acknowledgements

The authors would like to thank the organisations and participants involved in the experiments. This research was funded as part of the FP7 2012 Aeronautics and Air Transport programme under EC contract ACP2-GA-2012-314765-Man4Gen. The views and opinions expressed in this paper are those of the authors and are not intended to represent the position and opinions of the Man4Gen consortium and or any of the individual partner organisations.

REFERENCES

Air Accident Investigation Branch [AAIB]. (2007). Aircraft Accident Report 4/2007 - Airbus A340-642, G-VATL, 9 February 2005. Retrieved from: https://www.gov.uk/aaib-reports/aar-4-2007-airbus-a340-642-g-vatl-9-february-2005 .

Australian Transportation Safety Bureau [ATSB]. (2011). Inflight engine failure - Qantas, Airbus A380, VH-OQA, overhead Batam Island, Indonesia, 4 November 2010. Retrieved from: https://www.atsb.gov.au/publications/investigation_reports/2010/AAIR/AO-2010-089.aspx

Casner, S. M., Geven, R. W., & Williams, T. (2013). The effectiveness of airline pilot training for abnormal events. *Human Factors*, 55(3), 477–485

Dekker, S. W. A., Dahlström, N., Van Winsen, R., & Nyce, J. (2008). Crew Resilience and Simulator Training in Aviation. In E. Hollnagel, C. P. Nemeth, & S. Dekker (Eds.), *Resilience Engineering Pespectives: Vol 1 Remaining Sensetive to the Possibility of failure*. Aldershot: Ashgate.

Field, J., Fucke, L., Correia Grácio, B., & Mohrmann, F. (2016). Flight Crew Response to Unexpected Events: A Simulator Experiment. In AIAA Modeling and Simulation Technologies Conference (p. 3373).

Klein, G., Pliske, R., Crandall, B., & Woods, D. D. (2004). Problem detection. *Cognition, Technology & Work*, 7(1), 14–28.

Mohrmann, F., Field, J., Stoop, J. (2017). Resilient decision making in the cockpit: Does it work?. Proceedings from the 7th REA Symposium 26th – 29th June 2017.

Rankin, A., Woltjer, R., & Field, J. (2016). Sensemaking following surprise in the cockpit — a re-framing problem. *Cognition, Technology & Work, 18*(4), 623–642.

IMPROVING URBAN INFRASTRUCTURES RESILIENCE USING CONCEPTUAL MODELS: APPLICATION OF THE "BEHIND THE BARRIERS" MODEL TO THE FLOODING OF A RAIL TRANSPORT SYSTEM

Michaël Gonzva[1,2] and Bruno Barroca[2]
[1] SYSTRA, Innovation Department, 72 rue Henry Farman, 75015 Paris, France
[1] mgonzva@systra.com
[2] Paris-Est University, Lab'Urba Laboratory ("Génie Urbain" Department), Marne-la-Vallée, France
[2] bruno.barroca@u-pem.fr

Abstract

The vulnerability of guided transport systems facing natural hazards is a burning issue for the urban risks management. In this context, several conceptual models of resilience are elaborated for presenting the various possible resilience strategies applied to urban technical systems. One of this resilience conceptual model is the "Behind the Barriers" model based on the identification of four complementary types of resilience: (i) cognitive resilience; (ii) functional resilience; (iii) correlative resilience; (iv) organizational resilience. The purpose of this paper is to offer an application of this model to a specific urban technical system, a public guided transport system, facing a particular risk, a flood hazard. The paper is focused on a past incident on a French Intercity railway line impacted by a river flooding, in 2013. The level of resilience of this transportation line is assessed using the model both as an evaluation and action grid.

1. INTRODUCTION

Several facts and figures reveal the vulnerability of rail network systems facing different natural events, on an international scale. This vulnerability can easily be highlighted through the costs and the repair times of weather-related incidents. In 2006, for example, a 100-year flood event due to the rise of the Morava River occurred at the border of Austria and Slovakia. The flood affected an important line of the Austrian Federal Railways between Vienna and the Czech Republic along a section of around 10 km causing repair costs of more than EUR 41.4 million and a complete shutdown of passenger and freight operations for several months [Moran et al., 2010b, Kellerman et al., 2015]. Sandy storm in New-York in 2012 caused damages estimated at US$ 5 billion only for the metro and associated infrastructures [HCFDC, 2013]. As an overall picture at European scale, the research project WEATHER (Weather Extremes: Impacts on Transport Systems and Hazards for European Regions) showed that in terms of the cost assessment, floods caused more than EUR 103 million in damages to railway lines. This value can be compared with the damages on railway lines due to storm, about EUR 0.07 million, and due to snow and low temperatures, about EUR 0.04 million [Enei *et al*., 2011]. Therefore, the rail transport systems are indubitably vulnerable to many natural hazards and especially to flood events that imply extensive and expensive damages.

Furthermore, the modern cities are dependent on technical systems, considering them as critical infrastructures to ensure their functioning: transportation networks, electricity network, drinking water network, etc. Reducing the vulnerability of modern cities against natural hazards involves improving the resilience of these critical infrastructures, such as transport systems. For this purpose, examining the resilience of rail transport systems appears necessary to increase resilience at urban scale.

2. CONTEXT OF THE STUDY

In this dual context of need for mobility and natural hazards intensification, developing resilience-oriented approaches for analyzing critical infrastructures is became the new parading for the urban risk management since over the last decade. Numerous resilience conceptual models can be identified in the international scientific literature for analyzing urban technical systems facing natural hazards. These models can be classified into 3 main categories [Gonzva 2017]:

- Models aiming at building metrics for assessing resilience through criteria, indicators or required capacities;
- Models consisting in defining a comprehensive framework for shaping the concept of resilience into several complementary dimensions;
- Models characterizing resilience as a set of successive steps for any analysis.

Several pioneering and dominant models can be highlighted. Firstly, the 4R's Resilience Framework developed by [Bruneau et al. 2003], as a model based on metrics. This model divides resilience into 4 performance criteria:

- Robustness: the ability of elements to withstand a given level of stress or demand without suffering degradation or loss of function;

- Redundancy: the extent to which elements exist that are substitutable, meaning capable of satisfying functional requirements in the event of disruption, degradation, or loss of functionality;
- Resourcefulness: the capacity to identify problems, establish priorities, and mobilize resources when conditions exist that threaten to disrupt some element;
- Rapidity: the capacity to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption.

This approach is based on a measurable quantity which varies with time and is defined as the infrastructure's quality of service. This quantity can range from 0% to 100%, where 100% means no degradation in service and 0% means no service is available. Thus, measures dedicated to increasing the resilience of a system aim at improving the system's performance and/or decreasing the time to full recovery [Tierney & Bruneau 2007]. Many models have been developed as a spin-off from the 4R's Resilience Framework, in keeping with the idea of resilience quantification based on the robustness, redundancy, resourcefulness and rapidity [Chang & Shinozuka 2004; D'Lima & Medda 2015; Cimellaro *et al*. 2010).

Secondly, the City Resilient Framework (CRF) initiated and developed by [ARUP 2014] and the Rockefeller Foundation can dually act as a comprehensive framework and a model based on indicators. Indeed, according to the CRF, the urban resilience is based on the resilience of the urban systems characterized by 7 qualities:

- Reflective: reflective systems have mechanisms to continuously evolve, examine and systematically learn from their past experiences and will modify standards or norms;
- Robust: robust systems include well-conceived, constructed and managed physical assets, so that they can withstand the impacts of hazard events without significant damage or loss of function;
- Redundant: redundancy refers to spare capacity purposely created within systems so that they can accommodate disruption, extreme pressures or surges in demand;
- Flexible: flexibility implies that systems can change, evolve and adapt in response to changing circumstances through the introduction of new knowledge, practices and technologies;
- Resourceful: resourcefulness implies that people and institutions are able to rapidly find different ways to achieve their goals or meet their needs during a shock or when under stress;
- Inclusive: inclusion emphasizes the need for broad consultation and engagement of communities, including the most vulnerable groups;
- Integrated: integration and alignment between city systems promotes consistency in decision-making and ensures that all investments are mutually supportive to a common outcome.

Then, the model offers 12 key-indicators in order to assess the 7 aforementioned qualities. The CRF provides and interesting and comprehensive picture of urban resilience including all urban aspects. The CRF is also based on many and well documented past disasters that affected cities. Therefore, the CRF can currently be identified as one of the most relevant resilience model dedicated to cities and urban systems.

The objective of this paper is to provide a concrete application of a resilience conceptual model. The model has been identified in a previous review of the main and current resilience conceptual models realized by [Gonzva 2017]: the "Behind the Barriers" model. This model and its application to an urban technical system are presented in the following sections.

3. THE RESILIENCE CONCEPTUAL MODEL "BEHIND THE BARRIERS"

The resilience conceptual model "Behind the Barriers" (BB) is associated to urban technical systems such as transportation networks, wastewater networks, power supply networks, etc. According to [Barroca & Serre 2013], the model aims at guiding the implementation of resilience strategies and building a reference framework for mediation, exchanges and description of such strategies. These strategies should be regarded as part of the global management of natural risks affecting a city. Hence, the model is particularly suitable for the study of the natural hazards damaging urban critical infrastructures.

This conceptual resilience model required a given technical system and a given natural hazard. In this context, the model is based on the identification of four complementary types of resilience (Figure 1). More specifically, the cognitive resilience is the first pillar of the resilience insofar as knowledge about the risk and the needs of the impacted system and area during or after a crisis is absolutely necessary for drawing up relevant strategies for resilience. Based on this knowledge, the functional resilience, as the second pillar of the model, consists in maintaining the functioning of the system in order to provide the service during and after a crisis. Hence, functional resilience is implemented by working on reliability, increasing redundancy within the system, protecting the most critical components, etc. Beyond these two resilience dimensions so-called "barriers", the system is considered without sufficient protections in the case of a natural hazard occurrence. The correlative resilience corresponds to the capacity of getting correlation between the service providing by the potentially damaged system and the required use. Thus, during the crisis, the correlative resilience highlights the degraded level of service provided by system and the necessary adaptation of the demand (users, passengers, etc.). Finally, the organizational resilience expresses the capacity of local areas impacted by a crisis to mobilize general conditions or larger areas for the recovery. This fourth pillar of resilience is the capacity to promote post-damage recovery especially to technical systems by involving other cities.

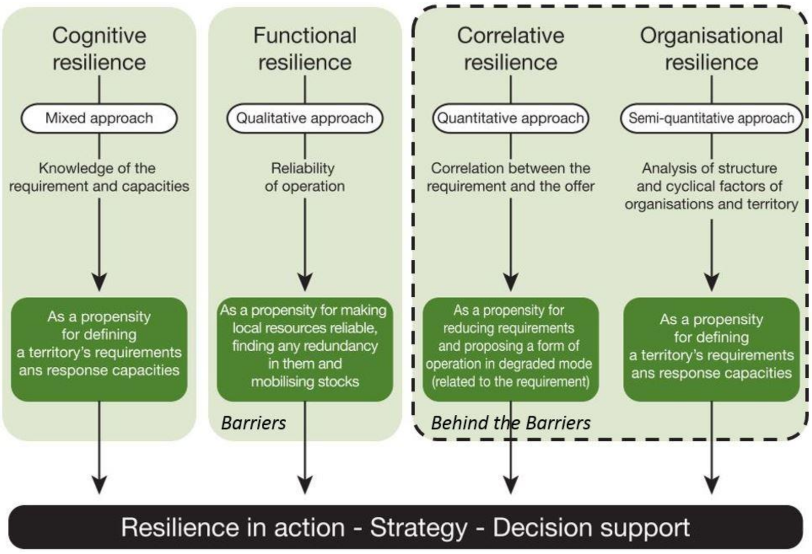


Figure 1. The conceptual model "Behind the Barriers" [Barroca and Serre 2013]

The model was applied to the public waste management during a post-disaster period: after the occurrence of a flood event. Indeed, during flooding, water degrades everything it touches, thereby producing very important quantities of waste. Thus, adapting waste management system and anticipating flooding contributes to improving urban areas' resilience. This is the reason why the model BB appeared relevant for this analysis of an urban technical system impacted by natural events [Beraud 2013].

4. APPLICATION OF THE "BEHIND THE BARRIERS" MODEL TO A FLOODED RAILWAY LINE

4.1. Description of the studied incident

On June 18th and 19th 2013 due to heavy rains, the rise of the level of the "Gave de Pau" river, located in the municipality of Coarraze, caused many disorders on the French Intercity railway serving the cities of Tarbes, Pau and Lourdes. The latter is knowing as one of the world's most important sites of pilgrimage and religious tourism during the summers. About 300 meters of the railway line has been damaged at Coarraze city:

- the flooding of the two tracks involving debris (Figure 2);
- the 80-meter collapse of the track slope : the ballast and the embankment;
- the collapse of a catenary pole on the track (N°1) involving the distortion of the catenary on the other track (N°2);
- a landslide of the track N°2 due to the flooding of the platform.

Figure 2. A picture of the railway line, on 18th June 2013 (photo credit : SNCF)

With a major constraint to reopen the line before August 15th, reinforcements were studied and applied in order to rebuild and stabilize the railway embankment. Indeed, although the Gave de Pau was still flooded and with a short time window (60 days) for works, the followings repair works were carried out [Ponchart & Chretien 2014]:

- The debris, mud and trees elements removal along the impacted section;
- The reconstruction of the embankment using rip-rap for reinforcing it against scouring and erosion;
- The removal and the reinstallation of the ballast and the tracks (rails, sleepers) on the embankment;
- The installations of new catenary poles.

During the works, a shuttle service has been provided by SNCF serving passengers going to and from Pau, Lourdes, Tarbes [La République des Pyrénées, 2013; Tisnès, 2013].

4.2. Application of the "Behind the Barriers" model to Coarraze incident as an evaluation grid: first step

Based on the resilience conceptual model chosen previously, an analysis of the flooding incident occurred at Coarraze is conducted. Indeed, the objective of such an analysis is to illustrate the capabilities of the BB model as an evaluation grid. To go further than just identifying the aspects relating to the four dimensions of the resilience, a rating is assigned in order to assess the quality of the cognitive, functional, correlative and organizational resilience of this railway line against flood events from overflowing rivers The four dimensions are qualitatively assessed using four categories: very low, low, high and very high (Table 1).

A representation of these qualitative assessment is offered using a radar profile (Figure 3). The surface area of the radar illustrates the number and the efficiency of the existing resilience strategies dedicated to the system.

Table 6. *Application of the "Behind the Barriers" four dimensions to the railway incident at Coarraze*

	Cognitive	Functional	Correlative	Organizational
Coarraze incident	Many previous disorders occurred: (i) a retaining wall was built in 1875 after erosions due to the river; (ii) a reinforcement was performed in 1966 after the river flooding; (iii) a closer surveillance was applied since 2012 due to sinkholes after flooding events. In 2013, a partial topographical mapping was made for getting information of internal damages.	As expressed through the cognitive resilience, many reinforcements of the railway line were performed. But, the regular flooding of the close river regularly provoked damages.	A shuttle service were set up by SNCF serving passengers. An efficient communication with users functioning has been implemented.	It can be mentioned that several local companies were involved during the reconstruction of the line. They were rapidly chosen due to the urgency of the rehabilitation.
Analysis	A strong historical knowledge of the risk exists on this railway line and reveals its vulnerability. But, in 2013, due to the repair time constraint, there was a low level of knowledge about required human and material resources.	Despite of civil engineering works for increasing the resistance of the embankment, the reliability of the line remains low. Besides, there is no other strategy implemented such as improving the overall connectivity of regional railway lines.	The capacity of bus shuttle was lower than the capacity of the railway line. Nevertheless, the service remained acceptable by users during the works period.	According to our survey based on newspaper articles and scientific papers, there was no particular mobilization of the local areas in order to accelerate the recovery of the railway line.
Rating	Very high	Low	High	Low

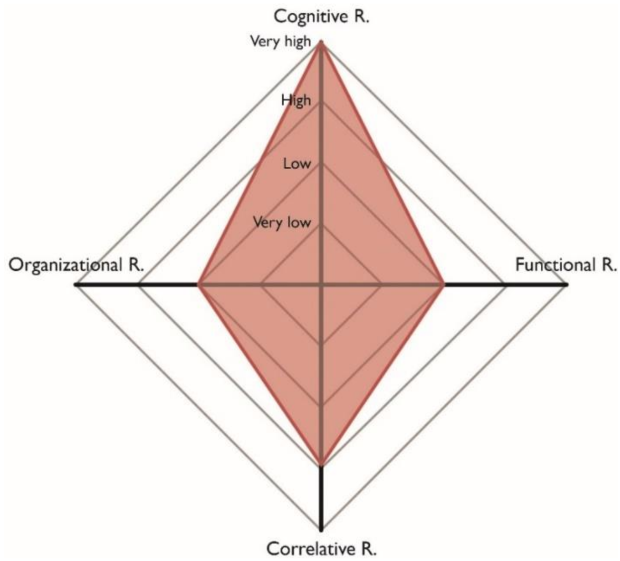


Figure 3. A representation of Coarraze incident assessment using "Behind the Barriers" resilience model

4.3. Application of the "Behind the Barriers" model to Coarraze incident as an action grid: second step

The second step allows by the BB model is focused on action. The first evaluation step provides a global view of the existing strategies available for technical systems' operators in order to increase the resilience on a system against one or several natural hazards. Then, a second step concerns the ability of the model to act as an action grid: this analysis highlights the aspects on which existing strategies are dedicated.

In the example developed in this paper, the first level of analysis using the BB model shows that the resilience capacity of this railway line against flood events is mainly composed of cognitive and correlative-oriented strategies. Therefore, in order to increase the resilience of this transportation line, the BB model reveals that the development of functional-oriented and/or organizational-oriented strategies could be very relevant.

In this context, other incidents occurred in the world on transportation lines and the risk management strategies implemented can be very useful. For example, in 2012, Sandy storm struck New-York city and particularly damaged the metro. In order to maintain sufficient level of mobility in the city, many organizational solutions were employed: between Brooklyn and Manhattan, 330 buses replaced the missing subway service (the so-called "bus-bridges") and ferry services to areas particularly hard-hit by the storm were increased or especially implemented with affordable prices during weeks [Kaufman *et al*. 2012]. Thus, the case of Sarry storm shows that the resilience of New-York city's overall transportation network is basically based on strong organizational-oriented strategies. Therefore, as indicated by [Barroca & Serre 2013], the BB model aims at conveying a common conceptualization, providing references for mediation, exchanges, and description; helping to develop a framework for analysis of the relevance of existing rules; and helping guide resilience strategies. In that case, the BB framework for resilience allows an identification and a transfer of good practices in terms of cognitive, functional, correlative and organizational-oriented strategies for resilience.

5. CONCLUSION

Rail transportation lines appear to be vulnerable to natural hazards and especially the flood events. The cities are highly dependent on these technical systems, considering them as critical infrastructures to ensure their functioning. Improving the resilience of cities against natural hazards can be efficiently obtained by improving the own resilience of these critical infrastructures, such as transportation systems. For this purpose, a lot of resilience conceptual models exist in the international scientific literature for conducting analyses of urban technical systems facing natural hazards. These models can be classified into 3 main categories: models aiming at using metrics for assessing resilience through criteria, indicators or required capacities; models consisting in defining a comprehensive framework for shaping the concept of resilience into several complementary dimensions; and models characterizing resilience as a set of successive steps for any analysis.

The objective of this paper is to illustrate the capabilities of a resilience conceptual model named "Behind the Barriers" from an incident occurred in 2013 on a French railway intercity line impacted by a river flooding. The level of resilience of this transportation line is assessed using the model as an evaluation grid on the one hand and as an action grid on the other hand. From the identification of four complementary types of resilience, the model aims at providing a common and operational-oriented conceptualization of the resilience, providing references for exchanges and description between stakeholders and helping to develop a framework for assessing existing rules. An interesting perspective could be now to go further into a quantitative way, meaning that the “Behind the Barriers” model could be used as evaluation and action grids thanks to a scoring of different options for improving the resilience of urban technical systems against natural hazards.

REFERENCES

ARUP. (2014). “City Resilience Framework.” London.

Barroca, B. & Damien, S. (2013). Behind The Barriers: A Resilience Conceptual Model. *S.A.P.I.EN.S*, April.

Beraud, H. (2013). Initier la résilience du service de gestion des déchets aux catastrophes naturelles - le cas des territoires urbains et de l’inondation. PhD thesis, Paris-Est University.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O’Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Kathleen, T., Wallace, W. A., & Von Winterfeldt, D. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, 19, 733–752.

Chang, S. E., & Shinozuka, M. (2004). Measuring Improvements in the Disaster Resilience of Communities. *Earthquake Spectra*, 20, 739–755.

Cimellaro, G. P., Reinhorn, A. M. & Bruneau; M. (2010). Seismic Resilience of a Hospital System. *Structure and Infrastructure Engineering,* 6, 127–144.

D’Lima, M., & Medda, F. (2015). A New Measure of Resilience: An Application to the London Underground. *Transportation Research, Part A: Policy and Practice,* 81. Elsevier Ltd, 35–46.

Enei, R., C. Doll, S. Klug, I. Partzsch, N. Sedlacek, N. Nesterova, J. Kiel, L. Rudzikaite, A. Papanikolaou, V. Mitsakis. (2011), *Deliverable 2: Vulnerability of transport systems - Main report*. Report prepared within the research project WEATHER funded under the 7th framework program of the European Commission.

Gonzva, M. (2017). Résilience des systèmes de transport guidé en milieu urbain : approche quantitative des perturbations et stratégies de gestion. PhD thesis, Paris-Est University.

Gonzva, M., Barroca, B., Gautier, P.-E. & Diab, Y. (2017). Modeling Disruptions Causing Domino Effects in Urban Guided Transport Systems Faced by Flood Hazards. *Natural Hazards*, 183–201.

Haut Comité Français pour la Défense Civile (HCFDC). (2013). *Retour d’expérience suite à l’ouragan Sandy sur la côte Est des Etats-Unis.* Paris. 92 p.

Kaufman, S., Carson Q., Levenson, N. & Hanson, M. (2012). Transportation During and After Hurricane Sandy. Rudin Center for Transportation, NYU Wagner Graduate School of Public Service.

Kellermann P., Schöbel A., Kundela G., & Thieken A.H. (2015). Estimating flood damage to railway infrastructure - The case study of the March River flood in 2006 at the Austrian Northern Railway. *Natural Hazards and Earth System Sciences*, 15, 2485–2496.

La République des Pyrénées (2013). *SNCF : la ligne Pau-Lourdes rouvrira "autour du 15 août"*, newspaper article published on July 17th.

Moran, A. P., Thieken, A. H., Schöbel, A., & Rachoy, C. (2010). Documentation of Flood Damage on Railway Infrastructure, *Data and Mobility*, 61–70.

Ponchart, I., & Chretien, M. (2014). Remise en état d’urgence du remblai ferroviaire de Coarraze après une crue majeure du Gave de Pau.” In: 2nd International symposium railway geotechnical engineering - GEORAIL 2014, 473–482. Marne-la-Vallée, France.

Tierney, K., & Bruneau, M. (2007). Conceptualizing and Measuring Resilience - A Key to Disaster Loss Reduction.” *TR News 250*, May-June, 14–18.

Tisnès, P.-M. (2013). Les trains sur de bons rails, *Sud-Ouest* Newspaper, published on August 9th.

THE EMBRACEMENT OF RISKS. HOW TO MAKE SENSE OF 'RESILIENCE' FOR PUBLIC AND INDUSTRIAL SAFETY?

Dr. Juul Gooren
The Hague University of Applied Sciences
Johanna Westerdijkplein 75
2521 EN The Hague, The Netherlands
jcwgooren@hhs.nl

Abstract

This paper will apply a generic definition of resilience ('the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances') to public and industrial safety. What can resilience teach us in terms of safety and security management? The avoidance of risk to ensure safety and security should not be the primary goal of a community or an organisation because that could undermine the primary processes of living in a community or working for an organisation. Safety and security is something that often develops indirectly as a result of involvement. It is under these conditions that a community or organisation will be more resilient. The prescription of 'simple, local and diverse' resonates as a response to the state-centred view on public safety and the tightly coupled and complex system in industrial safety. In order to be flexible resilience is sceptical of a central and hierarchical organization of safety and security. Furthermore resilience does not shy away from risk because risks offer all kinds of opportunities and gains. The purpose of this paper is to connect recent talk about building resilient communities with the work of resilience engineering. "*The capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances* (Zolli & Healy, 2012, p.7)"

1. INTRODUCTION

The notion of resilience seems popular these days (Comfort, Boin & Demchak, 2010; Ungar, 2012; Kent, Davis & Reich, 2014). Lentzos & Rose (2009, p.242) argue: "Initially an act of rebounding, recoiling or springing back: in the nineteenth century the term became applied to the capacity of a property or a structure to regain its initial shape after compression, and then, later, to the mental state of being able to withstand stress or adverse circumstances or to recover quickly from their effects, and, later still, to the capacity of systems, structures or organizations to resist being affected by shock or disaster, and to recover quickly from such events. Significantly, resilience, today, has become something that can be engineered into systems, organizations, perhaps nations and persons." One could apply this thinking to New York in the immediate aftermath of the 9/11 attacks when ordinary people started helping each other on the street (Molotch, 2012). It is also applicable to Wal-Mart which was fully operational after only one week in the areas hit by Hurricane Katrina (Tabot & Jakeman, 2009). In both cases whether it is laymen offering emergency assistance or alternative supply routes we are dealing with resilience for it signifies an "intentional stance of both fluidity (of strategies, structures and actions) and fixedness (of values and purpose) (Zolli & Healy, 2012, p.259-260)". See also Boutellier (2011) on the importance of improvisation bottom up in the delivery of safety and security.

I would like to apply resilience as a conceptual tool to understand the management of safety and security in the world of public and industrial safety. How can one improve the resilience of communities and organizations facing adversity? In dealing with risks I will elaborate on resilience as a different framework compared to on the one hand cost-benefit analysis and on the other hand precaution (Sunstein, 2005; Pieterman, 2009; Ball & Ball-King, 2011). In all its complexity the future is highly unpredictable and all the more due to interventions with unforeseen side effects (De Mul, 2014). The logic of resilience seems to be a fundamental preparedness no matter what (Weick & Sutcliffe, 2007). In order to locate this more recent approach in terms of interventions for safety and security problems I will draw on the safety and security management chain (Liebregts, 2011). Where to place resilience compared to well-known notions such as prevention and repression (O'Malley, 2010, 2011; Walklate, 2011; Walklate, Mythen & McGarry, 2012)? If resilience is a new approach in dealing with risks I am interested in the qualitative difference.

2. RESILIENCE

There seems to be a recurring set of elements explaining how certain systems are more resilient than others being too complex, concentrated and homogeneous (Zolli & Healy, 2012; Ungar, 2012; Kent, Davis & Reich, 2014). The most important elements often brought up are modularity, feedback and diversity. Modularity reduces vulnerability to any disruptions of wider networks that might cause cascading effects. Feedback is about detecting thresholds in a timely fashion in order to address little problems that have yet to become big. Diversity refers to the number of connections between stakeholders with a number of functions. The beauty but also problem of this framework is that is applicable to all kinds of situations. Let me give two random but recognizable examples. Think of a marriage between two people who respect individuality (modularity), communicate regularly (feedback) and seem to complement one another in all kinds of ways (diversity). A marriage can moreover change over time since it is possible that two lovers will eventually start a family and take up the role of parents alongside that other role of being romantic partners. The possibility to adjust and remain together implies upholding 'core purpose and integrity'. Think of a sports team with its inherent capacity to change the game plan during a match whenever being outclassed by an adversary. From a holistic point of view every player has its distinct role to play (modularity) and during a match one can often detect that things might turn out in a defeat because of little mistakes (feedback) requiring the substitution of certain players (diversity) as a real time strategy to keep up with changing circumstances. If a system is to be regarded resilient there are thus three important requirements. There must be autonomous subsystems, there is the ability to gather first hand data and difference is welcomed to the extent that various sources of knowledge and experience find their way into the decision making process. A resilient system is in constant need of refreshing resources for the immediate environment can always turn into a hostile one.

A resilient system remains dependent on a variety of interconnected and interdependent elements that are able to reconfigure whenever necessary. The field of complex adaptive systems covers similar terrain as resilience in its focus on diverse and autonomous components or parts which are interrelated, interdependent, linked through many (dense) interconnections and behave as a unified whole in learning from experience and in adjusting (not just reacting) to changes in the environment (Holland, 2005). With resilience we are not dealing with closure and protection for that will lead to homogeneity and paralysis. Resilient systems are much more open and dynamic and do not strive for homeostasis for they welcome change in the name of preservation. A resilient stance might require transformation. In similar vein Sennet (unknown, p.8) writes: "The boundary is an edge where things end; the border is an edge where difference groups interact. At borders, organisms become more inter-active, due to the meeting of different species or physical conditions; for instance, where the shoreline of a lake meets solid land is an active zone of exchange where organisms find and feed off other organisms. Not surprisingly, it is also at the borderline where the work of natural selection is the most intense." With a bit of imagination we can translate bio-diversity into socio-diversity thus replacing ecology with sociology. In resilient cities we typically find creativity and prosperity due to a mixed demographic and the possibility of encountering strangers leading to unexpected outcomes we tend to label as innovation. Following Ungar, (2012, p.27) "compensatory, promotive and protective processes contribute most to successful coping when individuals, families and communities face significant exposure to adversity." The logic of resilience advocates adaptation in addition to mitigation. It ultimately boils down to getting out of a comfort zone. Perhaps one can compare this to the effects of stress on the human body which is beneficial for health and safety for it is crucial considering the fight-flight response.

3. SAFETY AND SECURITY

Public safety is basically about living together as citizens. Crime and nuisance can be a problem for a community. Industrial safety is basically what organizations have to do in order to make sure that employees return home safely. In every type of organization accidents can happen because of work processes and human error. How to address both types of safety and security problems from a resilience point of view? The idea of liveability and productivity can be understood as the respective 'core purpose and integrity' of a community and an organization. The avoidance of risk to ensure safety and security should not be the primary goal of a community or an organisation because that could undermine the primary processes of living in a community or working for an organisation. Safety and security is something that often develops indirectly as a result of involvement (Crawford & Evans, 2012; Woods, 2006). Numerous authors argue that humans are innately capable of cooperation (De Waal, 2011; Sennett, 2012; Schuilenburg, Van Steden & Oude Breuil, 2014). It is under such conditions that a community or organisation will be more resilient. The success of responding to problems is very much dependent on social capital in the form of 'bonding', 'bridging' and 'linking' (Putnam, 2000). In the research I am now conducting I am most interested in 'linking' as "the extent to which individuals build relationships with institutions and individuals who have relative power over them (Hawkins & Maurer, 2010)". The notion of resilience seems to suggest more participation by residents and more opportunities for employee discretion might be the answer to safety and security problems. I believe a community police officer and a line manager could learn from one another in how to change human behaviour and create conditions to do so. My current study deals with the way these professionals work (Raaf, 2015). What both have in common is that they rely on those who are not professionally tasked with safety and security but who are nonetheless crucial considering their active role in the primary process. By focusing on active citizenship in a community and safety culture within an organisation I would like to discover how increasing resilience would work to promote safety and security within both communities and organisations.

If resilience is very much about cooperation than trust is crucial. Without trust there will be too much distance between the police and the residents and the same goes for higher management using a command and control layout for employees (Verhaege, 2015). It is this distance that will undermine the effective management of risk for there will be less exchange of information. Once exchange is no longer operative residents tend to withdraw from public space and employees tend to cover up faults (Jacobs, 1960; Heck, 2011). The archetypical example for living is the gated community making spontaneous encounters less likely (Sennett, unknown). A cubicle in which employees work dividedly on a joint project would be the archetypical example for working (Sennett, 2012). A closed off community or organization is vulnerable because of the limited amount of external contacts that might be necessary to solve problems. Whenever people are separated this is detrimental to involvement. The gated community and the cubicle resemble closed systems whereas resilience requires an open system. Just like active citizenship (Tonkens, Trappenburg, Hurenkamp & Schmidt, 2015) is about the meaningful and necessary immersion of residents, a mature safety culture (Hudson, 2007) is about employees carrying out what they know has to be done, not because they have to but because they want to. For the management of safety and security this means being sensitive to the primary process and involving the concerns of those affected. The 'simple, local and diverse' (Zolli & Healy, 2012, p.59-60) resonates as a response to the state-centred view on public safety and the tightly coupled and complex system in industrial safety. In order to be flexible, the logic of resilience is sceptical of a central and hierarchical organization of safety and security. In the case of public safety it is residents who have to perform social control and inform authorities. In the case of industrial safety it is employees who have to perform situational awareness and report near misses. It is this facilitation that resilience seems to promise.

In my research I will translate a resilient management of risk as the use of local knowledge and experience and the involvement of as many relevant stakeholders as possible resulting in safety and security serving a common interest. In a similar fashion as cost-benefit analysis resilience understands the management of risks as a trade-off (Hollnagel, 2009). Resilience is about balancing these trade-offs in order to reach an optimal result. The primary process should not be undermined by safety and security problems nor by the organization of safety and security. Here I am reminded of the school-to-prison pipeline exemplifying the 'securitization' (Zedner, 2009) of schools thereby overriding the goal of education because of zero tolerance policies and the presence of police (see Wacquant, 2001). In terms of resilience this means that safety and security authorities should respect the primary process of the social system in question. The best way to do that is to cooperate with the primary stakeholders such as residents and employees. More participation by residents relates to active citizenship. From a public safety perspective I have explored the function and organisation of neighbourhood watch groups which is a nice manifestation of residents exercising social control and informing authorities. These initiatives from and by citizens are aimed at decreasing crime and improve communities because of greater involvement. More opportunities for employee discretion relates to a mature safety culture. From an industrial safety perspective I will explore the work processes in an organization. Is the overall set up appropriate for employees exercising situational awareness and reporting near misses? Every employee can be exposed to risks and needs to report these if deemed substantial. By communicating information about the possible emergence of incidents more broadly the likelihood of risks materializing will diminish. In order to achieve this it is important that employees gain insight into their own work as it affects the work of others as well as the overall objectives of the organization.

4. APPLYING RESILIENCE

For all kinds of reasons the state's monopoly of security is being dispersed among various non-state actors. This relates to the market and to the community. In similar vein the management's monopoly of safety is being dispersed among lower level actors at the strategic, tactic and most importantly operational level who are more and more made responsible for safety and security management. Whether it is public or industrial safety the logic of resilience favors a bottom-up approach incorporating local knowledge and experience. On top of that resilience assumes that disturbances should not only be mitigated but also used in a productive way in that one needs to adapt.

In his classic study on searching for safety Wildavsky (1988) makes a distinction between anticipation and resilience. The former is about preventing danger not yet materialized (mitigation) whereas the latter is about dealing with danger (adaptation). This shift is clearly detectable in thinking about terrorist attacks post 9/11. No longer do authorities promise that such an event will not happen. Intelligence agencies do not have enough information or have too much information and cannot make sense of it. The question is not if, but where and when. The logic of resilience does not so much amount to intelligence agencies tracing the bad guy before he sets off a bomb (mitigation) but more importantly citizens reclaiming the streets after the bomb has exploded (adaptation). “If we cannot control the volatile tides of change, we can learn to build better boats. We can design and redesign organizations, institutions and systems to better absorb disruption, operate under a wider variety of conditions and shift more fluidly from one circumstance to the next (Zolli & Healy, 2012, p.5).” To continue operating under adverse conditions and circumstances refers to the ‘core purpose and integrity’ of a social system. In the case of international security and terrorist attacks that implies a curfew is perhaps a defeat for it undermines the liberty which is constitutive of being a US citizen. For industrial safety and accidents it is a defeat whenever a factory is completely shut down for this is rather inefficient when it comes to production. Finally whenever dealing with public safety and crime it is a defeat once gentrification leads to areas which are no longer lively in the sense that people from various backgrounds interact with one another. What these three examples have in common is that resilience is about tolerating a certain degree of risk that comes from living in an open democracy under the rule of law (international security), running a factory (industrial safety) and living in a diverse neighborhood (public safety). Moreover resilience argues one can learn from disturbances in that one needs to politicize conflicts (the field of human security), learn from mistakes (the field of resilience engineering) and value conflicts (the field of positive criminology). It urges safety and security managers to broaden their scope and be attentive to the respective primary processes that can actually benefit from disturbances. These can improve the overall quality of the social system. In the spirit of complex adaptive system theory Dekker (2006) argues resilience engineering is all about learning from mistakes as it is valuable for any organization. With a bit of imagination the same could be argued in the case of building resilient neighborhoods requiring conflicts as a means to strengthen norms and values (Christie, 1977).

I would like to argue resilience emphasizes the stages of pro-action and after-care as it is understood in the safety and security management chain. How to take away root causes and how quickly is it possible to return to ‘normal’? The chain of safety and security management consists of five stages in order to intervene in situations defined as risk (Liebregts, 2011). *Pro-action* implies taking away structural conditions with the aim of eliminating certain risks altogether. Think about the investment in education so youngsters follow the right path or on a different note replacing a dangerous machine as to make sure no one working in a factory loses a hand during the process of manufacturing goods. The stage of *prevention* is about taking measures of precaution to prevent unsafe situations and undesirable consequences. More technically this comes down to reducing risks. Think about stop and search policies and the placing of smoke alarms. Any intervention to stop and end an unsafe situation would qualify as *repression*. Think about a police arrest or extinguishing a fire. Another stage is *preparation* and that is basically the act of planning in case things go wrong. Think about scenarios related to riots or a fire drill. *After-care* finally is basically aimed at activities that will lead to reinvigorating the primary process. It implies getting better out of an adverse situation for lessons can be learned that can serve to enhance the subsequent stages. It is then that we have come full circle in applying the safety and security management chain.

5. CODA

Resilience should be understood as the capacity to deal with distinct events as well as latent processes for both are usually interrelated. Regarding distinct events like a riot (public safety) and an explosion (industrial safety) resilience is more about after-care whereas pro-action is more relevant in the case of latent processes such as ethnic tensions (public safety) and poor housekeeping (industrial safety) ultimately leading to these aforementioned distinct events. For me resilience is thus not only about 1) speedy recovery, 2) severe disturbances and 3) the capacity to remain functioning as Comfort, Boin & Demchak (2010, p.8) put it. It also includes 1) timely adaptation, 2) little disturbances and 3) the capacity to transform functions (ibid.). It implies there must be sensors in place that function as early warning signals that something is going wrong. From a resilience point of view trust and cooperation (Zolli & Healy, 2012) is something that is crucial in order to bounce back after a shock but should already be in place before the actual shock happened. It is something that should originate organically through social capital (Molotch, 2011; Waal, 2011) serving inclusive purposes and indirectly befitting the purpose of safety and security. From an empirical point of view resilience promotes a bottom up approach whereby those most closest to the primary process are able to ‘row’ and more importantly ‘steer’ (Wood & Shearing, 2007).

REFERENCES

Boutellier, H. (2011). *De improvisatiemaatschappij. Over de sociale ordening van een onbegrensde wereld*. Den Haag: Boom Lemma uitgevers.

Christie, N. (1977). Conflicts as Property. *British Journal of Criminology,* 17, 1-19.

Comfort, L.K., Boin, A. & Demchak, C.C. (2010). *Designing resilience. Preparing for extreme events*. Pittsburgh: University of Pittsburgh Press.

Crawford, A. & Evans, K. (2012). Crime Prevention and Community Safety. In: M. Maguire, R. Morgan, & R. Reiner (eds.), *Oxford Handbook of Criminology*. Oxford: Oxford University Press, 769-805.

Dekker, S. (2006). *The Field Guide to Understanding Human Error*. Hampshire: Ashgate Publishing Limited.

Hawkins, R.L. & Maurer, K. (2010). Bonding, Bridging and Linking: How Social Capital Operated in New Orleans following Hurricane Katrina. *British Journal of Social Work*, 40, 1777-1793.

Heck, M. (2011). Arbeidsveiligheid. In: W. Stol, C. Tielenburg, W. Rodenhuis, S. Pleysier & J. Timmer (red.), *Basisboek Integrale Veiligheid*. Den Haag: Boom Lemma uitgevers, 343-356.

Hollnagel, E. (2009). *The ETTO Principle: Efficiency-Thoroughness Trade-off*. Hampshire: Ashgate.

Hudson, P. (2007). Implementing a safety culture in a major multi-national. *Safety Science*, 45, 697-722.

Jacobs, J. (1961). *The Death and Life of Great American Cities.* New York: Vintage Books.

Kent, M., Davis, M.C. & Reich, J.W. (2014). *The resilience handbook: Approaches to stress and trauma*. New York: Routledge.

Lentzos, F. & Rose, N. (2009). Governing insecurity: contingency planning, protection, resilience. *Economy and Society*, 38, 230-254.

Liebregts, J. (2011). De ketenbenadering. In: W. Stol, C. Tielenburg, W. Rodenhuis, S. Pleysier & J. Timmer (red.), *Basisboek Integrale Veiligheid*. Den Haag: Boom Lemma uitgevers, 57-71.

Molotch, H. (2012). *Against Security*. *How We Go Wrong at Airports, Subways and Other Sites of Ambiguous Danger*. Jersey: Princeton University Press.

Mul, J. de (2014). *Domesticatie van het noodlot.* Rotterdam: Lemniscaat.

O'Malley, P. (2010). Resilient subjects: Uncertainty, warfare and liberalism. *Economy and Society*, 39(4), 488–509.

O'Malley, P. (2011). Security after Risk: Security strategies for governing extreme Uncertainty. *Current Issues in Criminal Justice*, 23(1), 5-16.

Pieterman, R. (2008). *De voorzorgcultuur. Streven naar veiligheid in een wereld vol risico en onzekerheid*. Den Haag: Boom Juridische Uitgevers.

Putnam, R. (2000). *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.

Raaf, H. (2015). *Voor de goede orde. Handhaven van wetten en* regels. Bussum: Uitgeverij Coutinho.

Schuilenburg, M., Van Steden, R. & Oude Breuil, B. (2014). *Positive Criminology: Reflections on Care, Belonging and Security*. The Hague: Eleven International Publishing.

Sennett, R. (2012). *Together. The Rituals, Pleasures and Politics of Cooperation*. New Haven: Yale University Press.

Sennett, R. *The Open City* (unknown). https://www.richardsennett.com/site/senn/UploadedResources/The%20Open%20City.pdf

Sunstein, C. (2005). *Laws of Fear: Beyond the Precautionary Principle*. Cambridge: University Press.

Tabot, J. & Jakeman, M. (2009). *Security Risk Management. Body of Knowledge*. New Jersey: John Wiley & Sons.

Tonkens, E., Trappenburg, E., Hurenkamp, M. & Schmidt, J. (2015) *Montessori-democratie. Spanningen tussen burgerparticipatie en de lokale politiek*. Amsterdam: Amsterdam University Press.

Ungar, M. (2012). *The Social Ecology of Resilience. A Handbook of Theory and Practice*. New York: Springer.

Verhaege, P. (2015). *Autoriteit*. Zutphen: Koninklijke Wöhrmann.

Waal, F. de (2011). *Van nature goed. Over de oorsprong van goed en kwaad in mensen en andere dieren*. Amsterdam: Atlas Contact.

Wacquant, L. (2001). Deadly Symbiosis: When Ghetto and Prison Meet and Mesh. *Punishment & Society*, 3-1, 95-133.

Walklate, S. (2011). Reframing criminal victimization: Finding a place for vulnerability and resilience. *Theoretical Criminology*, 15(2), 179–194.

Walklate, S., Mythen, G. & McGarry, R. (2012). States of Resilience and the Resilient State. *Current Issues in Criminal Justice*, 24(2), 185-204.

Weick, K.E. & Sutcliffe, K.M. (2007). *Managing the Unexpected. Resilient Performance in an Age of Uncertainty.* San Francisco: John Wiley & Sons.

Wildavsky, A. (1988) *Searching for safety*. New Brunswick & Oxford: Transaction Publishers.
Wood, J. & Shearing, C. (2007). *Imagining Security*. New York: Routledge.
Woods, D. D. (2006). How to design a safety organization: Test case for resilience Engineering. In: E. Hollnagel, D.D. Woods & N. Leveson (eds.), *Resilience engineering: concepts and* precepts. Aldershot: Ashgate, 315-324.
Zedner, L. (2009). *Security*. New York: Routledge.
Zolli, A. & Healy, A.M. (2012). *Resilience. Why things bounce back*. New York: Free Press.

FROM RESILIENCE TO ROUTINES AND BACK: INVESTIGATING THE EVOLUTION OF WORK ADAPTATIONS

Jop Havinga [1], Andrew Rae[1] and Sidney Dekker [1]

[1] Griffith University, 170 Kessels Road, Nathan Brisbane, Australia

[1] j.havinga@griffith.edu.au

Abstract

This paper explores how a routine shapes how small crews perform work. We investigated this on blast crews and power line crews, and will illustrate our findings with examples from the blast crews in mining. Literature generally describes routines as repeating action patterns, however, we found that there was a lot of variation between actions. We did find stability in how crews understood a problem and how they divided a task into sub tasks. The shared problem understanding and solution structure, provided sub-goals which crews could opportunistically act towards and enabled the creation of meaningful signals. These elements are returning between multiple iterations over time, but are subject to change as well. For development of resilience, this view of routines offers two possibilities, (1) the creation of routines that allows teams to deal with varying conditions and (2) the creating conditions that allow routines to change quickly over time.

1. INTRODUCTION

1.1. Significance of the Problem

No socio-technical system is fully pre-specified; people always have to fill in gaps. This is a sign of resilience: the ability to adapt fluidly to changing circumstances to meet production and safety expectations. However, when teams do the same task multiple times, they replicate things they have done before. People, teams, and systems in general, do not only respond to their goals and constraints but also have a path dependency. Their actions are at least inspired by, and often even structured around, what has been done in the past. We approach this phenomenon on the team level with the concept of a routine. Our research has explored the space between variation and replication in performing a task, the formation of a routine, and the change of routines.

1.2. Routines

Both safety and cognitive systems engineering literature refer to routines of teams. Klein, Feltovich, Bradshaw, & Woods (2005) say that the routines a team can perform form part of the common ground between members. Weick and Roberts (1993) regard routines as the opposite of heedful interaction. Snook (2000) and Vaughan (1996) both talk about how groups changing their routines over time is inevitable, but that without reflection on the changes, this can lead to accidents. These papers all consider routines important, but do not consider in depth what it means for a group to have a routine.

There is a diverse body of literature in organisational science on organisational routines. In this literature, routines have been linked to many things: routines reflect the skills and capabilities a team has, routines support coordination, routines capture a truce between competing goals, and routines are both inert and ever changing (Becker, 2004). The most common definition used for organisational routines is ‘‘repetitive, recognisable patterns of interdependent actions, carried out by multiple actors''. Routines here are viewed as a duality, consisting of a performative and an ostensive element. The performative element is the actions as done in a time and place, and as these actions or performed they imprint an ostensive image. The ostensive in turn provides a script of actions that guides the people when they perform the routine. Both parts are mutually constitutive, in that the parts form each other. Recognised challenges within this literature include that there is no clear explanation how actions in a routine link together (Pentland & Hærem, 2015) and that the line between variation within a routine and a change of a routine is difficult to identify (Feldman, Pentland, Adderio, & Lazaric, 2016).

1.3. Blast Crews & Powerline Crews

To investigate this, we studied both blast crews in mines and power line crews. Both blast crews and power line crews work do safety critical work, with partly interchangeable roles within crews. Both blast crews and power line crews bring their own equipment and practices to different working environments. In our research, we built and triangulated patterns with data from both types of crews. However, for communicative purposes, we will focus on blast crews in this paper.

Blast crews’ work in mines is to 'soften' up the ground. By using explosives they crush the ground, so that diggers in the mine have an easier job. If their blast is too weak, the rocks afterwards are too big. If their blast is too strong, environmental norms can be exceeded and debris can be flung away from the blast area. Besides debris, the job of blast crews is safety critical due to risk of premature and uncontrolled detonation, and managing risks that come with operating and working alongside heavy machinery.

Before a blast can be done, the area to be blasted is surveyed. After it is surveyed, a 'shot' is designed, which means a plan is made to decide what kind of explosive 'product' is used and how the product will be distributed around the area. The holes where the product will be loaded into are drilled per the plan. Next, the holes are filled. To fill a whole the crew first 'baits' the hole by lowering a booster (a small cylindrical explosive attached to a detonation cord into the hole. Then, the product is loaded into the hole and the hole is all topped off with stemming. The detonation cord sticks out of the top of the hole. The last step is to connect the detonation cords before the shot is set off from a safe distance.

2. METHOD

We conducted fieldwork for a total of seven weeks (usually with 12-hour shifts, excluding shared travel time) across different crews and different locations. The fieldwork consisted of observation, as well as semi-structured interviews about what people would do in different situations shown in pictures. The focus was on:

- How actions followed each other
- Differences and similarities between multiple instances of a task
- Differences and similarities within crews, between crews and between locations
- Changes over time in how people or teams would have addressed similar problems

3. RESULTS

While the routines literature described repeating patterns of actions, we found instead considerable variation in the patterns of actions of crews and crewmembers. Variation was both found in what actions were done and in the order of actions. There did not seem to be an ideal pattern of actions for a task, as individuals were often attuned to variations in the environment. Whilst crews and individuals did have predictable patterns in how they conducted work, these elements were not on the level of action sequences. The returning elements were in the things that produced the actions. These elements included:

3.1. Problem Space Understanding

The problem space understanding reflects what a person believes that needs to be done under what constraints. This includes the scope of work, what equipment is available, and how conditions affect the job. For example, in some mines crews had to border their working area, while in others this was done by other teams in the mine. Another example is that some crews would assume ground was wet and prepare accordingly, while crews would hardly ever encounter wet conditions and would only prepare if there were indications of wet conditions. This level builds on the experience of people and tends to converge for individuals in similar environments, as they have similar experiences. However, recognising the same problem does not mean the same solution is used to solve it, which refers to the next level.

3.2. The Solution Structure

This level is closest to how most literature talks about routines. The solution structure is about how work is divided into sub-goals or in-between-states to achieve shared across a team. This includes how the sub-tasks relate to each other and whether they need to be done in a particular order. The solution structure builds on the problem understanding but can vary between crews in similar environments. This exists on for high-level tasks, for example, at what moment a crew has a toolbox talk, as well as on a more detailed level, on what knot to use when tying up wires. Within a crew, there is a standardisation on what is achieved, not how crew members achieve this. A knot with which cords are tied up is standardised across a crew, but the technique used to produce that knot is not. Crew members will correct each other on deviating knots but are mostly oblivious to different tying techniques of fellow crewmembers. Allowing this variation in how to achieve sub-goals allows crew members to adapt to conditions.

Crews can know multiple ways of structuring the problem into sub-goals. For example, when loading a shot, the truck can move along the rows echelons. This fits with the idea that a team can roll out different routines.

On points where crew members interact, the sub-goals of different crew members tend converge within a team. However, this does not mean the division of the problem into sub-tasks is exactly the same for an entire team. For example, with measuring the water depth of a hole and writing it on a peg next to the hole, novices tended to divide the task into more and smaller steps with a constant order, while experts would adapt order of the steps based on what gear and information were closest at hand. Here experts did not roll out an 'ideal' or 'ostensive' pattern of actions, instead they responded opportunistically towards the sub-goals. Experts can also add more steps to the process than novices do. For example, experts might spend more time in a preparation phase to look for challenges. In general, however, experts were more sensitive to sub-goals further down the track, while novices were mostly guided by immediate sub-goals.

Having shared sub-goals facilitates that the work of individuals together solves the whole task. The stability in these sub-goals facilitates the establishment of meaningful signs within crews, which in the next level of a routine.

3.3. Established Signs:

A shared problem understanding and shared solution structures with standardised sub-goals (in-between-states) enables the formation of meaningful signs within a crew. The problem understanding can help in the way that Peirce (Flach, 2015) describes that a signifier is interpreted in relation to a problem domain. For example, a dewatering truck and inflatable bags can signal an operator that a crew is dealing with wet in holes, but an operator from a crew that works in dry areas, might not recognise this equipment and not relate this to wet conditions.

Standardised sub-goals create quickly recognisable signs, even when the signifier does not directly relate to the problem understanding. For example, one crew would park a car at the point they planned to finish that day. None of the other crews had this practice, so people from other crews would not give this meaning to the location of the parked car when they viewed pictures of this crew at work, but they would recognise the car was 'weirdly' parked in the path of the truck.

Standardisation of in-between-states also enables deviance to become a sign. When tying up wires on a blast side, team leaders tend to be specific about which way they want the wires connected and are very particular about how they want leftover cords to be organised. This is not because they consider their way superior, but by having cords laid out according to a standard, unintended slips would easily be spotted during the check-up process. With no standardisation, the team leader would have to follow each wire individually to determine whether the wires would ignite the right way. The standardisation allowed him to trade computational demands for perceptual demands, as in moving from knowledge-based processing to rule or skill based processing in the S-R-K framework (Rasmussen, 1983). Deviance from the norm would function as a sign that things were not done as intended.

Deviation was also used as a sign intentionally. If blast crews would run into a problem with a hole, they would often mark the hole with whatever was closest at hand. This could things as placing a stone across the hole, marking it with spray paint, or tying a bag to the peg next to the hole. Different signifiers could have the same meaning, and the same signifier could have different meanings, in different phases of work. Even tough the signifier varied, by relating it to what work had been done in an area to the solution-structure as well as the problem understanding, they could typically interpret these signals. If they could not, they would ask fellow crewmembers why a hole was marked. Some crewmembers specifically mentioned that this adaptiveness in markers was required. Specific markings for specific problems, like coloured ribbons, had been tried, but this approach was found not to work. People would not run into problems when it was not expected and not have the right markers at hand. Without the right markers, a hole would have to be left unmarked, at least till the right marker was organised, which could take up to 20 minutes if it was at the depot. The paradox here is that standardisation facilitated crews to be adaptive with their markers.

3.4. Change of Routines:

So far we have talked about what replicates in routines - what crewmembers take along between multiple iterations of a task. While these elements show permanence, they are not completely static. Small changes are common and often go unnoticed, especially if a change does not affect other parts of the work. However, one change would often feed into other changes in the routine. For example, cardboard holders were introduced to blast crews to prevent material from rolling away. Expectedly, crews added putting out these holders next to holes into their routine, and it when putting out gear, and new acceptable in-between-states had the gear inside these holders. Unexpectedly, some crews would turn these holders upside down if they encountered problems with a hole, a practice that developed from these cardboard holders now often being the closest thing at hand.

While routines did not specify actions within a crew, we did see routines change by instructing actions. For example, from management there had been the instruction to tie loose cords into a bundle, to prevent people from tripping over it. Across crews this same instruction led to different knots, creating differences in acceptable in-between-states between crews. Also, some crew would knot the cords after check up, which turned the knots into a sign that the holes had been checked. While the action of tying up loose cord was instructed to multiple crews, it led to different sub-goals and different signals across crews.

4. CONCLUSION AND TAKEAWAY

The actions of a team can quickly change if the environment changes. However, there was consistency in the problem understanding, a division of the problem space into sub-goals, and signs. On the level of actions towards these sub-goals, however, crewmembers to responded to local conditions and acted based on what was available. These elements are carried over through between enactments and show permanence between enactments, but can change over time.

To support team resilience, this offers two paths. One is to create routines that can handle more situations; the other is to facilitate the change of routines. To build routines that can handle a wide range of conditions, for this the problem understanding and solution structuring should be as shared as possible within a crew and develop a redundancy of established sign. For this, teams are best kept stable, while they encounter varying conditions. To facilitate the change of routines, goal feedback should be visible, interaction between people with different problem understandings and solution structures should be encouraged, and the signifiers need to get a different meaning overtime. Exchange of practitioners between crews is beneficial for all of these elements.

Acknowledgements

This research is part of a larger research project funded by ORICA. The views presented are those of the authors and should not be taken to represent the position or policy of the funding bodies.

REFERENCES

Becker, M. C. (2004). Organizational routines: A review of the literature. *Industrial and Corporate Change*, *13*(4), 643–677.

Feldman, M. S., Pentland, B. T., Adderio, L. D., & Lazaric, N. (2016). Beyond Routines as Things: Introduction to the Special Issue on Routine Dynamics. *Organization Science Publication*, *27*(3), 505–513.

Flach, J. M. (2015). Supporting productive thinking: The semiotic context for Cognitive Systems Engineering (CSE). *Applied Ergonomics*, 1–13.

Klein, G., Feltovich, P. J., Bradshaw, J. M., & Woods, D. D. (2005). Common Ground and coordination in joint activity. In W. B. Rouse & K. R. Boff (Eds.), *Organizational simulation* (pp. 1–42). Hoboken, NJ, USA: John Wiley & Sons, Inc.

Pentland, B. T., & Hærem, T. (2015). Organizational Routines as Patterns of Action: Implications for Organizational Behavior. *Annual Review of Organizational Psychology and Organizational Behavior*, *2*(1), 465–487.

Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *… , Man and Cybernetics, IEEE Transactions on*, (3), 257–266.

Snook, S. A. (2000). *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*. Princeton, NJ: Princeton University Press.

Vaughan, D. (1996). *The challenger launch decision: risky technology, culture, and deviance at NASA*. Chicago, US: The university of Chicago Press.

Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, *38*(3), 357–381.

FROM AIR TO GROUND – RESILIENCE STRATEGIES AND INNOVATION ACROSS CRITICAL INFRASTRUCTURES

Ivonne Herrera [1] and Beth Lay [2] and Karen Cardiff[3]

[1] SINTEF, Department of Software Engineering Safety and Security and Norwegian University of Science and Technology (NTNU), Department of Industrial Economics and Technology Management, Trondheim, Norway

[1] ivonne.a.herrera@ntnu.no

[2] Applied Resilience, 404 Emerson Street Houston TX, US

[2] elizabeth.a.lay@hotmail.com

[3] Consultant, Health Care, Vancouver, British Columbia, Canada

[3] kcardiff498@gmail.com

Abstract

We compare strategies and tactics for increasing resilience in three critical domains: aviation, healthcare, and energy. We explore similarities and differences adressing the following questions: What does resilience look like in everyday operations in an air traffic control center, a power plant control room and an acute care hospital? How does each setting anticipate, prepare and respond to surprising and novel events? Are there strategies that are uniquely suited to each domain, and why? Which strategies would work across domains? Which would not and why? The authors disclose a self-serving motive of learning from each other thereby building a richer toolbox for resilience engineering practitioners. The themes will consider the challenge of implementation and thus be paired with innovation techniques that could be used to co-create robust solutions with end-users. This creates an opportunity for innovative thinking at all levels of the organization with respect to preparing for, and responding to novel and surprising events. Management innovation to mature resilience concepts gives room for unique and unorthodox approaches to unleash people's thinking and attitudes; where everybody is pushed to consider useful solutions.

1 INTRODUCTION

Demographic and socio-economic changes, globalization, fast-paced technological innovation with an increasing reliance on automation and access to digital data, all have a significant impact on the way that people think about and perform their work. How does the workplace reconfigure itself to respond to these changes to ensure continuous operation and provision of essential functions and services? We start with the underlying theme that systems today are very complex, and yet both management and frontline staff can be resilient and adaptive to the dynamic and often unpredictable nature of everyday work. Our challenge is to understand the resilient and adaptive capacity of high-risk, complex workplace environments, with the overall goal of developing a platform to enable resilient and adaptive capacity. We begin by highlighting the complex nature of three risk critical industries and then we describe what is currently understood about the key features of resilient teams. Following this, we explore the potential of applying innovation management and innovation games to enable resilient and adaptive capacity in the workplaces.

2 COMPLEX ADAPTIVE SYSTEMS AND WORKPLACES

Air traffic management is an example of a complex system. It is a formal system, with clear roles and responsibilities defined by international rules, regulations, manuals and procedures adapted to different aerodromes. Air Traffic Controllers have a range of responsibilities, including providing air-space control and guidance to the aircraft under varying conditions e.g. seasonal, weather, interactions with other air traffic management units as well as coordination with other organizations such as ground services and airline companies. Cyber-physical systems and increase of automation are transforming operational concepts and ways of working towards highly networked systems-of-systems. An example is remote tower operations.

Modern power plants epitomize complex systems and variable work. "Everyday work" in power plants has been disrupted with the increase in renewable power, plants that were once "base-loaded" (running constantly) are now starting and shutting down daily; work happens on elevated platforms, in all kinds of weather, in hot, enclosed spaces, and everything in between. One mechanic described routine work as "It's different every time." Complexity comes from the many, interconnected and interrelated systems that make up a power plant with critical, tight operating parameters and little margin for error.

The delivery of healthcare is also marked by complexity and unpredictability. Diversity is a key feature of health care delivery – diversity of patients, diversity of clinical specialization and support staff, diverse and often complex care pathways, and the trajectory of patient care often involves a range of locations with substantial variation of the clinical layout and care environment. The social context of healthcare is also complex, as patients are inherently vulnerable and there are a myriad number of relationships to manage – between patients, healthcare providers, support staff, family members and community agencies. There is rapid implementation of new technologies. In healthcare, work situations are always underspecified (i.e. the conditions of work frequently do not match what has been specified or prescribed), and thus when unpredictable components or dynamics arise within the system, adaptation is often necessary. Performance variability is both a normal and necessary feature of the healthcare setting.

3 CURRENT AND EMERGING RESILIENCE THEMES ("PRIMER FOR RE NOVICE")

3.1 Resilience Organizational Characteristics

Drawing from bodies of knowledge in Resilience Engineering (RE), Highly Reliable Organizing (HRO), and our own experiences, we paint a picture of "ideal" resilient teams, they:

- *Are prepared to be surprised. Point of view: surprise will happen.* They notice and manage small signals, emerging risks, and uncertainty. They practice making decisions when uncertainty is high. They look for how they will be or have been surprised. They prepare for the general shape of risk.
- *Hold a constant sense of unease*. *Point of view: past performance is not an indicator of future success.* Remaining sensitive to the possibility of failure or opportunity is recognised as important both within High Reliability Organizational (HRO) theory and RE (adapted from Hollnagel, Nemeth & Dekker, 2008).
- *Are flexible, adaptable, and gracefully extensible (positive capability to stretch near and beyond boundaries when surprise occurs). Point of view: change is constant.* They develop adaptive capacity (ability or potential to adjust activities, resources, tactics, and strategies in the face of different kinds of events, variations, demands, and uncertainty) to regulate processes relative to targets and constraints. This is a simple extension of an old definition for skill and expertise, the ability to adapt behaviour in changing circumstances to pursue goals (Woods lecture on Resilience Engineering, 2015). They prepare both static (margin) and dynamic (capacity) slack, defined as available, spare resources of any sort which can be called on in times of need (Freyer, 2004). They manage differently when close to boundaries. Systems and organizations need graceful extensibility as a separate kind of capacity to our everyday performances when the system is far from the boundary conditions (Woods, 2015). *Sustained adaptability* offers new ways to manage interdependencies across scales. It refers to the ability to manage adaptive capacities of systems (organizations) that are part of a layered network (Woods, 2017 in preparation).
- *Learn on a routine basis from every day activities, threats as well as opportunities. Point of view: Important lessons are in the 99% of work that goes well.* Learning focuses on frequency, performance variability and performance adjustments during every day work. They also learn from situations where something unexpected happened, uncertainty was high, operating close to boundaries, or running out of margin to respond through assessing how well and quickly they dealt with the situation.
- *Are empowered at local level with humble leadership. Point of view: workers are local experts.* Organizing for resilience requires a balance between local and central governance. Through humble leadership and empowering people with necessary expertise to solve the situation at hand, resilient organizations provide space for creative problem solving. Leaders leave rank at the door and commonly offer help to the frontlines.
- *Understand the distance between work as imagined (WAI) and work as done (WAD). Point of view: work is variable.* Conditions related to the work, worker, and workplace are always changing. Workers are afforded freedom and flexibility to get their job done, guided by commander's intent. Routine work is approached looking for what's different today. The people who write the rules and procedures make the effort to understand the challenges faced by the front line.
- *Value different points of view and are collaborative, cooperative. Point of view: it takes variety to manage variety.* They build capabilities to manage responses within work units and across different levels of the organization. They create opportunities to build relationships and offer help across organization boundaries. They create insight into each other's responsibilities, challenges, and goals. They employ practices to look from different perspectives (more experienced-less experienced, challenger, outsider, and details-big picture). During shift changes, trouble shooting, and assessing risks, there's a lot of back and forth engagement wherein they invite cross checks and ask clarifying questions. (Rayo et al, 2013)

- *Pay attention to the system within its boundary and its environment. Point of view: the system is complex, interconnected, and interdependent.* They plan how to handle relationships, interactions, different tempos, non-linear dynamics, and hidden dependencies; "thinking outside the box" (strategic foresight) is key. They study and plan how they'll handle failure patterns or opportunities. They look for tight couplings that increase brittleness then loosen or de-link, if possible.
- *Use safety models that fit complex socio-technical systems. Point of view: focus on the presence, not the absence, of safety.* A possibility is to analyse functions of how organisations work (e.g. FRAM, Hollnagel, 2017) to change focus from individuals towards resilience performance. When an event emerges, they seek to understand the perspective of those involved and the conditions that existed; moving away from linear, cause and effect models. The interest is to capture, understand and the way systems work when challenging changes occur. It also considers set of organizational aspects: formal systems; technology; values and knowledge in the organization; interactions; and social relations (e.g. Pentagon Model, Schiefloe at al., 2005).

3.2 Why innovation as enabler for resilience management?

We've just described significant changes in perspective from traditional safety programs. We suggest that it takes innovation to successfully implement the non-traditional ideas that RE brings. Innovation management can support the creation of something that is both novel and useful when established rules and procedures no longer apply. In this section, we offer ideas on applying innovation management which have been applied in different European projects.

Innovation can be large or incremental (Mckeown, 2014; Hill, et al, 2014). We relate this innovation process to graceful extensibility, as it can be a new process or a new way of organizing or a creative solution to solve the problem or opportunity at hand.

Today´s complex adaptive systems (CAS) require a multidisciplinary problem solving approach where decision-making is deferred to expertise (Dekker, 2014); Weick & Sutcliffe, 2007). Engaging team members with relevant expertise that includes knowledge about operational processes and sensitivity to how work gets done on the frontlines is a critical feature of managing threats and opportunities. The challenge is to how to successfully engage team members in this process. Each person in the team contains a relevant expertise that need to be collected, combined and converted into viable solutions. We see innovation as a core process which needs to be organized and managed to enable renewal of an organization. The concern is not to build a strong innovation management capability but to acknowledge the challenge to create a learning and adaptive approach which constantly upgrades the dynamic resilience capabilities associated with survival and growth (adapted from Tidd and Bessant, 2009). We use innovation management practices and innovation games to create space where people are willing to collaborate, experiment and integrate ideas and co-create solutions. Specifically, we establish shared values amongst team members and this create an environment where people is willing to collaborate and co-create solutions (Hill et al, 2014). These values are as: (1) To address complex challenges, foster experimentation, learning, improvisation and structure; (2) Collaboration of diverse people, with the involvement of end users (operational, maintenance personnel and managers) who interact closely, consolidate ideas and make integrative decisions; and (3) Learning through collaboration and discovery, encouraging diverse and even conflicting views.

We adapted storytelling and innovation games such as the ones proposed within "gamestorming" (Gray, D. et al., 2010). Stories are defined as "narratives with plots and characters, generating emotion in the narrator and audience, through a poetic elaboration of symbolic material. This material may be a product of fantasy or experience, including an experience from earlier narratives. Story plots entail conflicts, predicaments, trials, coincidences, and crises that call for choices, decisions, actions, interactions, whose actual outcomes are often at odds with the characters intentions and purposes" (Gabriel, 2000). The innovation games enable the creation of "new worlds" exploring everyday operations, challenging situations or introduction of new technologies, analysing systems and organizations opportunities and challenges improving collaboration and generating new insights about the way these "new worlds" works and what kind of possibilities we can find there (Gray, D. et al., 2010). Table 1.0 describes a set of innovation games used in different contexts, highlighting the respective purpose and relation to resilience management.

Table1: Example of innovation games adapted to explore resilience

Method (M) – Game (G)	Purpose	Relation to resilience	Lessons learned
Storytelling (Gabriel, 2000)	Rich source of material, not a reliable source of information but it can be revealing. It reveals that facts cannot reveal, individual, peoples or groups value.	Narratives as way of knowledge sharing	Narrative can lead to discoveries
Affinity Map (G)	Discover patterns and meaning by clustering information into relations	organization practices	Used to understand resilience in action. Participants map concepts to their own stories.
4C (Components, Characteristics, Challenges, Characters) (G)	Rapid way to gather and organize information	operational resilience capabilities	Good to map relevant stakeholders and capabilities at managerial and operational level
The Blind Side (G)	To disclose and uncover unknown information	performance variability	Effective way to gather variables affecting performance
Training for resilience capabilities (TORC) (Grøtan et al, 2016)	To guide operational teams and management teams to recognise and facilitate resilience as a critical capability in the context of compliance	sense making, anticipation, respond and after action review	Potential application areas everyday operations, emergency planning, unexpected situations

Our experience so far shows that storytelling and innovation games are powerful tools allowing all participants to share their views and knowledge. We have so far used them for training, discovery of resilient performance and evaluation. We see future areas of application addressing improvisation and creativity during times of surprise for example adapting the "blind side" game mapping and updating "things we know, we know and things, we do not know" during events, thus creating a window of opportunity for action.

4 CROSS INDUSTRY PRACTICES TO INCREASE RESILIENCE ("HOW TO GUIDE")

A key idea in RE is the importance of "everyday work" in creating resilience. Below we share practices that support creating resilience.

Table2: **Sample practices from each domain featured, arranged according to selected characteristics**

Theme	Air Traffic Management (ATM)	Power Plant	Health Care
Are prepared to be surprised.	Update on airport current conditions, update on recent developments before starting work. Do simulations involving surprises as part of certification program.	Pretask briefs: "What's different that could make it harder or easier?" "When we did this in the past, what surprised us?" After Action Reviews: "What surprised us?"	Change of shift, intensive care units. IDRAW I= identify patient; D= current problems; R=recent changes; A=anticipated changes; W=What to watch for? (i.e. What should I be most worried about?). (Wrae Hill, 2015)
Hold sense of unease : Past performance is not an indicators of future success	Briefings are part of hand-over. Actively, constantly monitoring the situation both within the ATM and its surroundings considering potential bottlenecks or opportunities ahead.	Set tone prior to high risk tasks (ex. rotor lift "if you notice anything, no matter how small – stop. Trust your intuition.") Plan detailed monitoring when starting up after major overhaul.	Patient safety huddles: mid-shift briefings that create heightened awareness of both staff and patient needs throughout a shift, opportunity to clarify information, anticipate what could go wrong, and manage staffing issues.
Are flexible, adaptable,	Support colleagues in case of overload. People available with	Avoid scheduling critical work during holidays when have fewer people working.	Prepared to shift people for the "unexpected" such as environmental disasters or

Theme	Air Traffic Management (ATM)	Power Plant	Health Care
gracefully extensible	different competences that can take different roles if required. ATM has many redundant systems	Schedule "NASA hold point" near end of difficult maintenance project to re-center and address any issues before hitting "restart" button. Have few redundant systems since risk of equipment tripping is generally accepted.	threats such as chemical spills or earthquakes, riots, terrorist attacks, epidemics. Overcapacity protocols to manage overcrowding in emergency departments; development of "rapid assessment zones" to reduce overcrowding in emergency departments
Learn on a routine basis	Situations occurred in one site are shared with other sites. Normally focus learning from unwanted situations. Probe where things are going well, ask "where do we never experience (this problem)? Why is that?" (Lundhal, 2016) Do simulations involving surprises as part of certification program.	Share case studies between plants that tell story, from point of view of those involved, to just before revealing what happened, ask: "What would you do? How could this play out? What would you do to avoid…?" Do After Action Reviews when things go well.	Learning through critical incident investigations. Regulatory bodies establish standards and create opportunities for learning. Simulation based learning (artificial representation of a real world process (e.g. clinical scenarios) to achieve educational goals).
Are empowered at local level with humble leadership	Supervisors adapt and reconfigure sectors to shift load… to cope with changing demands and challenging conditions.	Remove symbols of rank (ex. parking places at front, special place at the table). Develop scenario training based on common sacrifice decisions, define acceptable level of risk tolerance. (Crandall, 2000)	Healthcare delivery is strongly hierarchical, and this can be a barrier to effective communication. Leadership can actively work to flatten hierarchy, minimize power distances, and consistently engage all team members.
Understand the distances between work as imagined (WAI) and work as done (WAD)	Air traffic controllers actively monitor each other. Air traffic controllers and supervisors practice "humble inquiry" (Schein, 2013)	Teach value of, and how to ask, open-ended questions. (Schein, 2013) Implement "Learning Teams" wherein you query WAI and WAD (Hollnagel, 2017, Conklin 2012)	Critical incident investigation work that uses a framework based on resilience perspectives. Patient safety senior executive walk-arounds to understand how the work gets done on the frontlines.
Value different points of view, collaborative, cooperative	In the control rooms collaboration between controllers, supervisors and novices is practiced considering the criticality of the operation. This builds trust necessary to perform reconfiguration and adapt to situations.	Purposefully build cross-plant relationships. Drill with all staff to build understanding of each other's roles and develop trust. Teach collaborative engagement during shift turnover: taking turns, off-going invites crosschecks, on-coming actively questions. (Rayo, 2013)	
Pay attention to the system	Operational personnel look to the system and relation	Look for tight couplings and interdependencies, loosen	Critical incident investigation that

Theme	Air Traffic Management (ATM)	Power Plant	Health Care
	to their environment e.g. other actors.	or de-couple (ex. brittleness assessment when planning multiple maintenance outages). Notice patterns, such as a plant trip followed brief lull before 2nd cascade begins.	understands safety as an emergent property of the system, and seeks to explain the system level contributions to incidents, rather than looking solely at the sharp end of care.
Use safety models that fit complex socio-technical systems : How safety is created is more important than the absence of safety	For new technologies, different safety models are in experimentation. Case studies analyse the impact of new technologies on ways of working (e.g. remote towers). Resilience perspective enables identifying bottlenecks as well as new ways of using technology.	Create safety through learning to notice "stack-up of risks", recognizing risk and uncertainty through language (ex. "worse than", "not sure"), and Real Time Risk Assessments for quick response for emergent risks. After an incident, seek to understand conditions, dilemmas, and system view.	Overcapacity protocols to manage overcrowding in emergency departments; the development of "rapid assessment zones" to reduce the potential of overcrowding in emergency departments

5 DISCUSSION

All three domains (ATC, power plants, and healthcare) implement methods to understand incidents from system and 2nd story points of view, consider social aspects of work, such as value of using open ended questions and developing humble leaders and shift people or roles to expand capacity. All prepare for surprise through simulations and drills. ATM is in a high state of alert almost continuously, while power plants and healthcare have specific briefs wherein they question and crosscheck related to higher risk work or patients. ATM develops resilience through many redundant systems (note that redundancy could be more related to robustness than resilience), this is less common in power plants and healthcare.

Opportunities for ATM and healthcare include learning from how they have been surprised on a routine basis. Healthcare has routinized shift handovers to probe where to focus attention for oncoming; this practice would benefit both ATM and power plants.

6 CONCLUSIONS

We presented a set of resilient characteristics relevant to three critical infrastructures. We propose the use of both established organizational methods such as storytelling and unorthodox tools such as innovation games to support identification of these characteristics and resilient practices. We have used our experience to reflect how resilience is part of everyday operation in different domains. This knowledge has been collected through years of practice, interview data, observations, questionnaires, storytelling and application of innovation games. We conclude that both adaptation of existing and innovation management tools support a paradigm shift to a resilience-oriented perspective based on RE and complemented by other relevant fields of research and practice.

REFERENCES

Conklin, T. (2012) *Pre-Accident Investigation and Introduction to Organizational Safety.* Boca Raton, FL: Taylor and Francis/CRC Press.

Crandall, B, Klein, G. & Hoffman, R. (2000). Working Minds: A Practitioner's Guide to Cognitive Task Analysis. Cambridge, MA: MIT Press.

Fryer, P. (2004). Running an organization along complexity lines. In: Kernick, D. (Ed.) Complexity and Healthcare Organization: a view from the street. Abington: Radcliffe Medical Press. 289-298.

Gabriel, Y. (2000). Storytelling in organizations. Oxford: Oxford University Press.

Gebauer, A. (2013). Mindful organizing as a paradigm to develop managers. Journal of Management Education. 37(203)

Gray, D. et al. (2010). Gamestorming: A playbook for innovators, rulebreakers, and changemakers. O'Reilly M.

Grøtan TO, Wærø I, van der Vorm JKJ van der, Beek FA van der, Zuiderwijk DC, (2016). Using gaming and resilience engineering principles to energize a situated resilience training of front-end operators and managers.

ESREL, Glasgow, Scotland.

Dekker, S. (2014) Deferring to expertise versus the prima donna syndrome: a manager's dilemma. Cognition, Technology and Work archive. Vol. 16, p. 541-548 . Springer, UK

Fryer, P. (2004). Running an organization along complexity lines. In: Kernick, D. (Ed.) Complexity and Healthcare Organization: a view from the street. Abingdon: Radcliffe Medical Press. 289-298.

Hill, L., Brandeau, G., Truelove, E., Lineback, K. (). Collective genius: the art and practice of leading innovation. Harvard Business Review Press.

Hollnagel, E., Nemeth, C. P. & Dekker, S. (2008). Remaining sensitive to the possibility of failure (Resilience Engineering Perspectives Volume 1). Aldershot, UK: Ashgate.

Hollnagel, E. (2017). Safety II in practice: developing resilience potentials.

Lay, E. (2011). Practices for Noticing and Dealing with the Critical. A Case Study from Maintenance of Power Plants. Resilience Engineering in Practice (pp. 127–144). Farnham, UK: Ashgate

Lay, E., Branlat, M., Woods, Z. (2015). A practitioner's experieince operationalizing resilience engineering. . In C. Nemeth & I. Herrera (Eds.). RESS. 141. http://dx.doi.org/ 10.1016/ j.ress.2015.04.006.

Lundhal, M. (2016). "Runway incursion prevention – a Safety II approach" Hindsight, Issue 24(46 – 49)

Mckeown, M. (2014) The Innovation Book. Pearson.

Rayo, M., Mount-Campbell, A.F., O'Brien, J.M., White, S. E., Butz, A., Evans, K. & Patterson, E. (2013). Interactive questioning in critical care during handovers: a transcript analysis of communication behaviors by physicians, nurses and nurse practitioners. BMJ Quality and Safety. 23(6)

Schein, E (2013). Humble Inquiry: The Gentle Art of Asking Instead of Telling. San Francisco: Berrett-Koehler.

Schiefloe, P.M. et al. (2005) *Årsaksanalyse etter Snorre A hendelsen 28.11.04*. Stavanger: Statoil

Tidd, J., Bessant, J. (2009) Managing Innovation: Creating Technological, Market and Organizational change. John Wiley & Sons, Ltd.

Van Dalen, B., Slagmolen, R. & Tang, R. (2009). Mindful Organizing: How to Manage Unexpected Events and Unwanted Processes. Nijmegen, Netherlands: Apollo Publishing.

Weick, K.E. & Sutcliffe, K.M. (2007). Managing the unexpected: Resilient Performance in an Age of Uncertainty. San Francisco: Jossey-Bass.

Woods, D.D. (2015) "Four concepts for resilience and the implications for the future of resilience engineering,"

RESILIENCE ENGINEERING - HOW TO HANDLE THE UNEXPECTED

Stefan Hiermaier, Sandra Hasenstein and Katja Faist[1]

[1] Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, Eckerstr. 4, 79104 Freiburg, Germany

[1]hiermaier@emi.fraunhofer.de

http://www.emi.fraunhofer.de/en.html

Abstract

Resilience engineering is concerned with the design, construction and operation of critical infrastructures aiming at abilities like disaster tolerance, quick recovery and adaptation. Quantitative measures to assess the resilience of a given system refer to this ability via time integrals describing the loss performance after a disruptive event.

There are two characteristics of disruptive events typically challenging the resilient design of critical infrastructure. First uncertainty, they often happen to an unexpected time or in an unanticipated way. Second, due to the ever rising complexity and inter-connectedness of the involved systems, their potential to initiate cascading effects is big. As a consequence, a classical threat-based approach for the resilient configuration of a system potentially misses its design goal if neglected sources of harm lead to a disruption.

Being used to outlay a system based on threats with given loads and boundary conditions, engineers easily find themselves in a dilemma if confronted with the task to deliver a resilient design for the unexpected. This paper discusses an approach utilizing generic damage scenarios as one option to go beyond classical threat-based concepts.

1. INTRODUCTION

Resilience engineering is concerned with the design, construction and operation of critical infrastructures aiming at abilities like disaster tolerance, quick recovery and adaptation. The criticality of an infrastructure is given if a system or a facility is essential for the maintenance of vital societal functions [Council of the European Union (2008)]. Supply chains, communication grids or transport infrastructure as well as financial or security services are typical representatives.

Engineers adopted the resilience concept introduced in the late seventies of the last century by psychologists [Werner, (1977)] in order to extend the classical perception of safety and security. According to Biringer et al. (2013) "… the infrastructure security community in the United States and globally recognized that it was simply not possible to prevent all threats to all assets at all times." The engineering concept for resilience of critical infrastructures takes into account the residual performance of a damaged system after a disruptive event as well as time and efforts needed to recover. As a result, a combination of classical security steps with post-damage activities is provided within the so-called resilience cycle (Figure 1) containing the characteristic phases of prepare-prevent-protect-respond-recover.

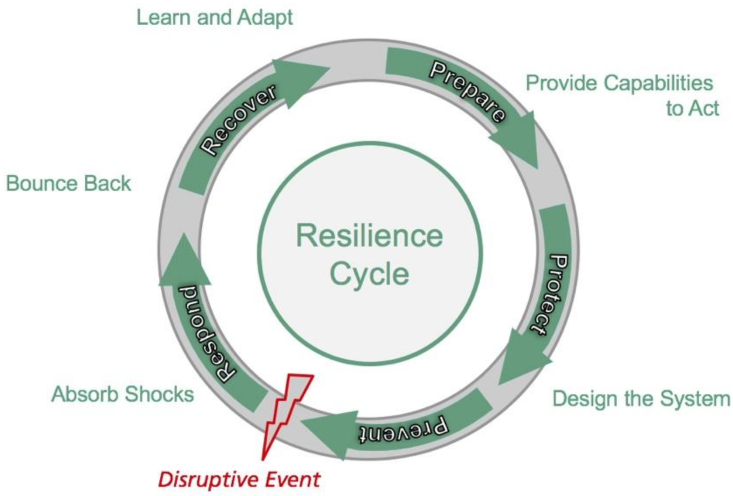


Figure 1. *Five-phases resilience-cycle*

Different measures have been derived to quantitatively assess the resilience of a given system [Tierney &

Bruneau (2007), Bruneau & Reinhorn, (2006), Vugrin et al. (2014)]. If a system is expected to deliver a performance at a certain level $P_{initial}$ (see Figure 2), a disruptive event leads to a drop of this performance. The deviation from the expected standard performance, calculated as time-integral and marked as "Performance Loss" in Figure 2, can be used to asses the resilience of the system. The smaller the performance loss, the higher the level of resilience. Moreover, observing the time history of the performance of a system across the initiation of the disruptive event also allows for directly linking the phases of the resilience-cycle to this type of resilience measure.

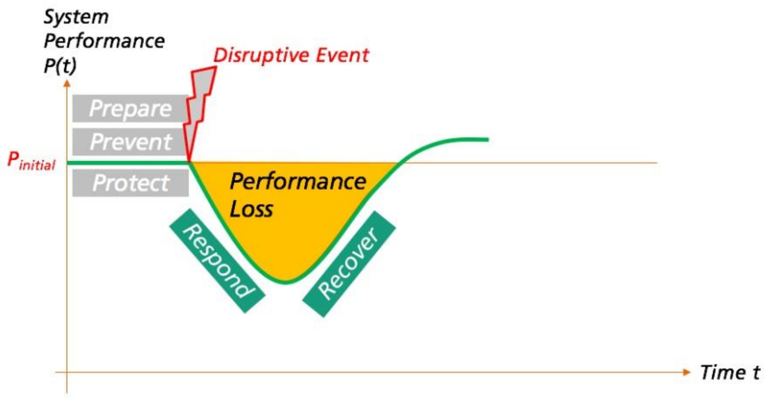


Figure 2. *Time history of system performance and performance loss as measure for resilience.*

The illustrated integration of response- and recovery-phases into engineering design is the novel contribution of resilience ontop of classical safety and security research. The time history of both the response path and the recovery branch allow for a quantitative measure of resilience.

Thus, following the paradigm of the psychologists, engineers for good reason focus on the ability of technical systems to recover from adverse conditions and to adapt based on experience. There are two characteristics of disruptive events typically challenging the resilient design of critical infrastructure.

- First, they often happen to an unexpected time or in an unanticipated way.
- Second, due to the ever rising complexity and inter-connectedness of the involved systems, their potential to initiate cascading effects is big.

As a consequence, a classical threat-based approach for the resilient configuration of a system potentially misses its design goal if neglected sources of harm lead to a disruption.

Being used to outlay a system based on threats with given loads and boundary conditions, engineers easily find themselves in a dilemma if confronted with the task to deliver a resilient design for the unexpected.

To overcome this dilemma, a modified concept for resilience engineering incorporating the unexpected is needed. This paper discusses an approach utilizing generic damage scenarios as one option to go beyond classical threat-based concepts. Considering the topology of the resilience cycle, the new concept is an approach starting from potential consequences rather than from threats.

2. OBJECTIVES

Modeling software has become an important tool to analyze the multi-physics behavior of complex systems. Pederson et al. (2006) is often cited for their collection of existing modeling tools for interdependent infrastructures as well as for their graphical and matrix-based illustration of interdependencies between grids of different types. Propagation of failure in multi-domain grids is investigated by Hover (2011) where a mathematical methodology for an asymptotic model of cascading failure in two-domain coupled infrastructures is proposed. In his PhD thesis, Rahman (2009) addressed a wide range of grid types with a numerical formulation implemented in his infrastructure modeling and simulation framework called "I2Sim". A detailed overview on different modeling approaches for critical infrastructure is collected and discussed in Attoh-Okine (2016).

Engineers are used to apply numerical and analytical codes to design and optimize technical systems. Given the complexity of critical infrastructures and the wide range of possible consequences after local disruptive events, a software based approach to design a systems and to investigate its behavior under critical loads is desirable.

Ideally, a design and assessment tool for resilient infrastructures would cover a range of capabilities like:

- modelling the physical components of the system including their interactions

- definition of an intended system performance
- calculation of the current system performance and comparison with expected performance
- definition of load cases resulting from specified disruptive events
- definition of generic damage scenarios, i.e. event-independent damage scenarios
- calculation of consequences to the overall system performance
- identification of critical system components and damage scenarios
- assessment of the resilience of the system
- implementation of mitigation strategies towards more resilience
- re-calculation of system resilience including mitigation strategies

With these functionalities implemented, engineers are enabled to design and assess the resilience of complex technical systems. Two characteristics of the software tool are important with respect to the before mentioned dilemma for engineers.

First, the physical and potentially multi-physical domain of the infrastructure is modelled in terms of components for which a well-known set of analytical or partial-differential equations is applicable.

Secondly, an option for event-independent, generic damage scenarios allows to better prepare for the unexpected. The ability to simulate a certain damage effect, regardless of the initiating reason, gives rise to more independence on actual events.

A new software tool, called CaESAR, incorporating some of the above mentioned functionalities has recently been developed at Fraunhofer EMI. It is designated to the simulation of multi-grid systems.

3. METHODOLOGY

3.1. Software Tool CaESAR

CaESAR is a coupled grid simulation tool, which computes cascading effects within grids and across grid borders to assess and enhance the resilience of critical infrastructures in urban areas. The overall target is to find optimized strategies for the mitigation of crisis impact on inter-connected grids. Considered are three critical grid types – the power grid, the water grid and the mobile phone grid. For this purpose, the CaESAR tool is connected to a dashboard, where the grids are mapped in terms of nodes and arcs in a geo referenced map. From this map CaESAR takes all information to calculate sensitivities, vulnerabilities and levels of resilience of the grid system. A crisis editor is used to define a damage event.

There are two types of damage to be implemented in CaESAR:

- threat-based damage resulting from events like natural disasters and
- generic damage, defining a threat-independent damage scenario, e.g. local or global power grid failure.

Both types of damage scenarios may be defined as single ones or in combination with others. The chronological sequence and interval of single events can be defined in the crisis editor. For every single event an intensity can be set by choosing low, medium or high.

Figure 3 illustrates the major definition and computational steps within the CaESAR tool. Having defined an initial damage scenario, CaESAR simulates its propagation into the grid systems. A standard method for propagating the damage impact inside a supply grid, e.g. within the power grid, is a flow model. CaESAR also provides interfaces to use third-party propagation models. Since these third-party tools are specialized for a specific grid type, their results tend to be more accurate. For propagating the damage impact between different grids, specified physical models are used. These models also utilize geo references and a defined dependency radius estimating possible interaction between different grids.

The damage propagation is used to computationally determine the resulting damage on the entire system of grids. It starts with a sensitivity analysis taking into account probabilities of component failure and is followed by a calculation of related failure mechanisms. The result of both is the residual performance level of the coupled supply grids after the disruptions. And, thus, the input for a later calculation of the resilience level R taking into account the initial and the residual performances, respectively. The analysis is iterated with variations in the probabilities for the sensitivity analysis. With these parameter variations, critical components and failure mechanisms are identified as the ones which happen most often or with most severe consequences.

A resilience value R for the coupled grids is computed in the next step. For the before identified critical components, the CaESAR tool proposes mitigation strategies. To this end, a limited set of predefined mitigation measures is implemented. Its application leads to changes in the performance level of the overall grid system. This new level is not necessarily higher than the one without mitigation strategies. Therefore, the resilience estimation is performed once more based on the mitigated status leading to a resilience value R_M.

Finally the two resilience levels R and R_M are compared and new simulation run can be started if needed.

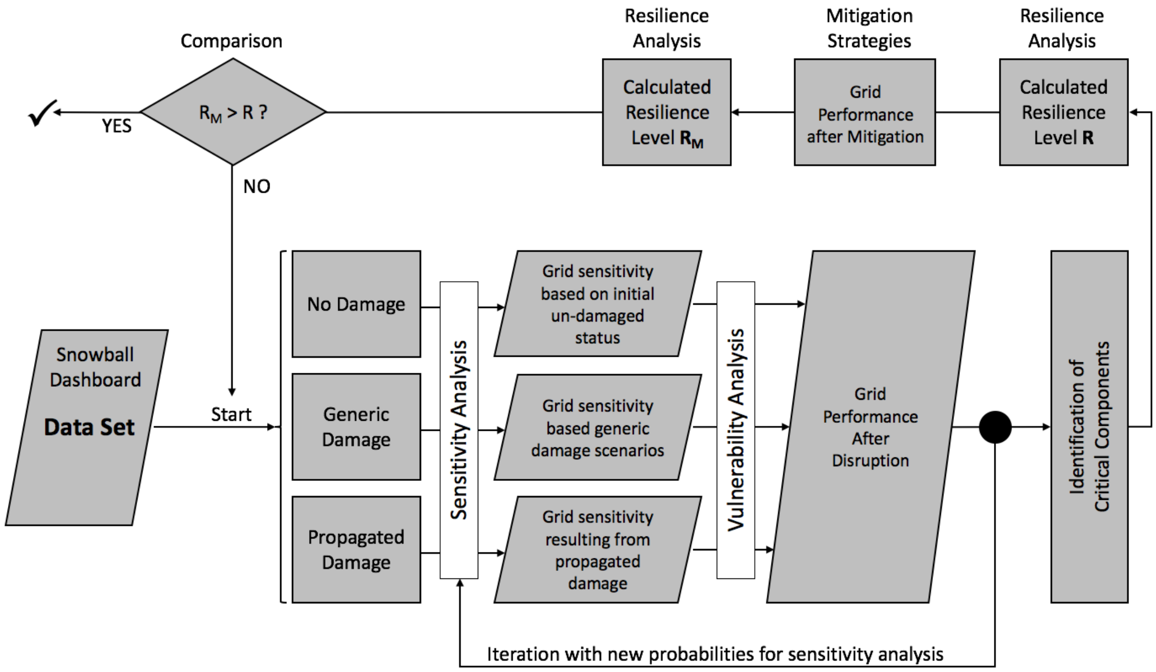


Figure 3. *Flowchart of the CaESAR tool.*

3.2. Set Up of Helsinki Urban Multi-Network Environment

An urban environment near Helsinki was chosen as an example application of the CaESAR tool. For the Helsinki grids shapefiles, which are suitable to share GIS information, were utilized. The shapefiles were attached to and presented in the map on the dashboard (Figure 4).

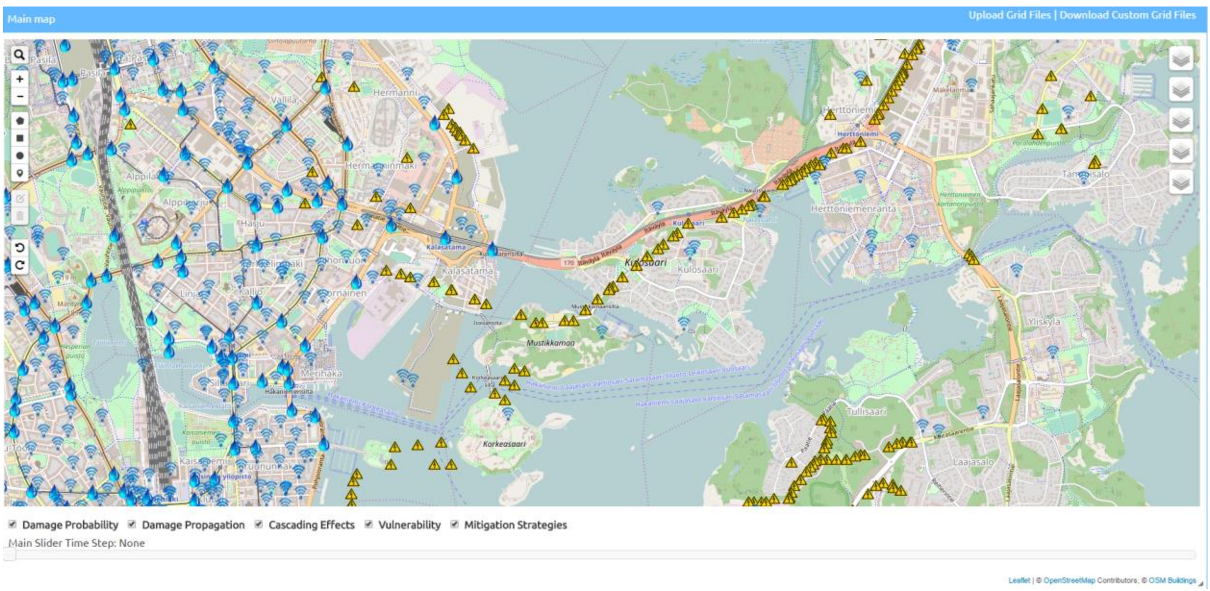


Figure 4. *Helsinki model including grids for power supply (yellow flash symbol), water (blue drop symbol) and mobile communication (blue radio symbol).*

With the dashboard, damage scenarios including threat-based and generic damage can be implemented. Illustrated in Figure 5 is the damage scenario resulting from a storm on the south coast of Finland. Using the map, the location of the storm, its start and end time as well as its impact strength are defined. Based on the grid data and the damage definition the calculation run of CaESAR starts.

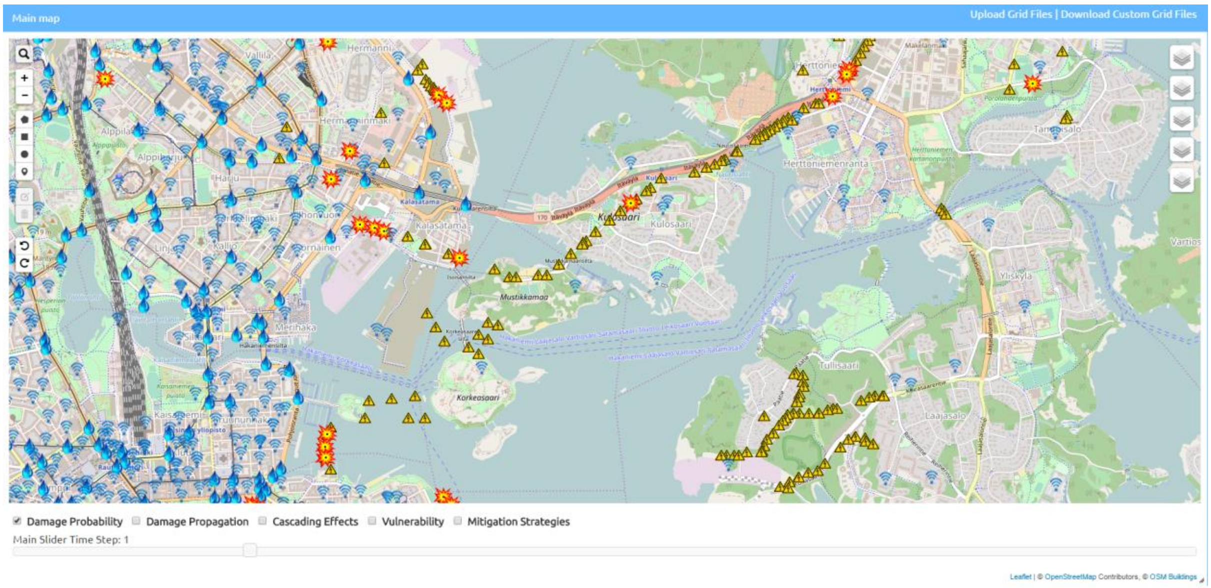


Figure 5. *Damage scenario resulting from coastal storm (red-yellow marked).*

4. RESULTS

Applied to the Helsinki scenario, the CaESAR tool provided a variety of critical components as well as mitigation strategies to increase the resilience level for the envisaged damage scenarios.

In general, there are now three major results to be gained using the CaESAR tool:

- A resilience measure for interconnected supply grids resulting from threat-based or generic damage scenarios
- Identification of the most critical components within the supply grids
- Assessment of mitigation strategies to increase the resilience of interconnected supply grids

The damages and the damage propagation based on the pre-defined chronological sequence and interval of single events during the crisis can be displayed on the map on the dashboard in several time steps.

Currently, a limited set of mitigation strategies can be applied to grid components. There are three different mitigation strategies implemented in the CaESAR tool: structural strengthening, installation of redundant components and an integration of an uninterrupted power supply. Structural strengthening and the installation of redundant components are applicable to all of the three grids. An uninterrupted power supply can be applied to water and mobile phone grid components, only.

5. DISCUSSION AND CONCLUSION

With the development of CaESAR, complex interconnected supply grid systems can be modelled. A quantitative resilience assessment based on system performances before and after a disruptive event is performed. The disruptions to the grid system can be defined as threat-based or generic.

With this approach, a first step towards damage-based and threat-independent design for resilient performance is achieved. The unexpected nature of many resilience-critical disruptive events can, thus, be addressed.

Still, CaESAR has its current short-comings. One of the next steps should be the implementation of more types of grids as components of critical infrastructure. Another field of further development is identified in more and more flexible mitigation strategies.

REFERENCES

Attoh-Okine, N.O., (2016). Resilience Engineering. Models and Analysis. Cambridge University Press, NY.

Biringer, B., Vugrin, E. & Warren, D. (2013). Critical Infrastructure System Security and Resiliency. New York: CRC Press.

Bruneau, M. & Reinhorn, A.M. (2006). Overview of the Resilience Concept. In *Proceedings of the 8th US National Conference on Earthquake Engineering*, number 2040, 2-6.

Council of the European Union (2008): COUNCIL DIRECTIVE 2008/114/EC of 8 December 20018 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In Official Journal of the European Union. L345 (pp. 75-82)

Hover, F. (2011). Degree Design of Coupled Infrastructures. International Journal of Critical Infrastructures, 7:2, 141-162.

Pederson, P., Dudenhoeffer, D., Hartley, S. & Permann, M. (2006). Critical Infrastructure Interdependency Modeling: A Survey of US and International Research. Technical report. Idaho National Laboratory, 25, 27.

Rahman, H.M.A., (2009). Modeling and Simulation of Interdependencies Between the Communication and Information Technology Infrastructure and Other Critical Infrastructure. PhD Thesis, The University of British Columbia.

Tierney, K. & Bruneau, M. (2007). A Key to Disaster Loss Reduction. *TR News*, 16-18.

Vugrin, E., Baca, M., Mitchell, M., & Stamber, K. (2014). Evaluating the Effect of Resource Constraints on Resilience of Bulk Power System with an Electric Power Restoration Model. *International Journal of Systems of Systems Engineering,* 5(1), 68-91.

Werner, E. (1977). The Children of Kauai. A longitudinal study from the prenatal period to age ten. University of Hawai'I Press.

TOWARDS AN OPERATIONALIZEABLE DEFINITION OF RESILIENCE

Samuel W. Huber [1] and Thomas Kuhn [2]

[1] Forventis, Wildbachstrasse 50, 8008 Zürich, Switzerland

[1] huber@forventis.ch

[2] armasuisse, Feuerwerkerstrasse 39, 3602 Thun, Switzerland

[2] thomas.kuhn@armasuisse.ch

Abstract

Background: Often, resilience is being regarded as a homogenous concept, valid to be applied in various domains. This led to rather broad and diffuse definitions that can be difficult to operationalize. There exists a deductive and an inductive understanding of resilience. Unfortunately, there are several drawbacks to the deductive view as it is possible that a non-adaptive system shows a typical resilient response behavior, while a truly adaptive system may show a degrading performance that has nothing in common with a typical resilience performance curve. The inductive view may overcome some of these problems.

Results: Resilience emerges in a state of overload. Overload occurs, as soon as performance requirements exceed the response capabilities of a given system. Resilience is defined as the capability of a system to stay productive in an overload state and to overcome the overload state through adaptation. A resilient reaction can be differentiated into a degrading and an adaptation phase. We've found specific principles, capabilities and mechanisms that enable the emergence of resilience.

Conclusion: The Framework presented could serve as guidance towards an operationalization of resilience in socio-technical systems.

1. INTRODUCTION

The concept of resilience is becoming widely used by many industries where safety and security is crucial for success. Often, resilience is being regarded as a homogenous concept, valid to be applied on individuals [Meredith et al., 2011], projects [Kutsch, Hall & Turner, 2015], organizations [ASIS SPC.1-2009], C2 systems [Pflanz & Levis, 2012], supply chains [Kim, Chen, Linderman, 2015], government [Homeland Security, 2014] or even societies [United Nations, 2017] equally well. This popularity led to rather broad and diffuse definitions that are sometimes difficult to operationalize.

Not only being a term in colloquial language, the term resilience is widely used by the life sciences [Freitas & Downey, 1998], social sciences [Ayling, 2010] as well as management science [Välikangas, 2010], not only with different foci but often with different meanings. Resilience as a concept originated within ecology [Walker & Salt, 2006] and is also applicable in the realm of socio-technical systems. The concept of resilience has a rich history, sometimes with a considerable stretch from its original meaning [Gallopin, 2005].

Principally, there are two different approaches towards a definition of resilience. The typological (or deductive) approach focuses on resilience as a response characteristics to a shock or disturbance and therefore on the "expression" of resilience that can be visualized as typical response curve. It is often referred to because of its easy and rather intuitive accessibility [Prior & Herzog, 2013].

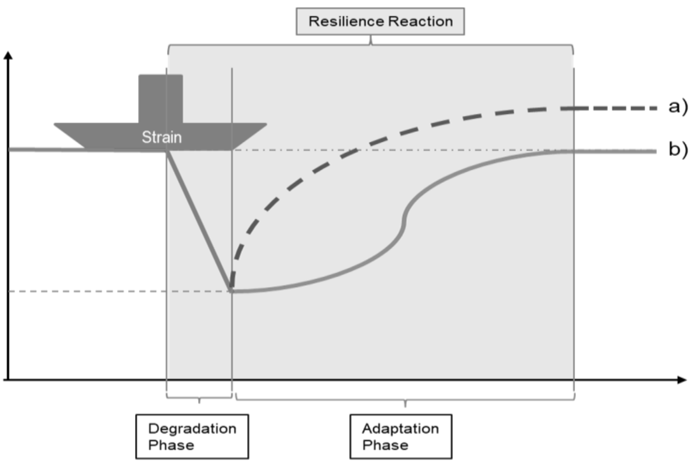


Figure 1. *Expression of resilience: typical response curves: a) "Bounce back" b) Adaptation*

However, there are several drawbacks to this perspective of which the inherent ambiguity is probably the most significant one. Following the typological approach, it is well possible that a completely non-adaptive system shows a typical resilient response behavior, while, on the other hand, a truly adaptive system may show a degrading performance that has nothing in common with a typical resilience performance curve. Therefore, this a posteriori definition is not necessarily useful for an a priori model to build up resilience from first hand. The second approach is the taxonomic (or inductive) approach which may overcome some of these problems but is not as intuitively accessible as the typological one [Gibson & Tarrant, 2010]. However, for this paper we will focus on the taxonomic approach and limit the scope of our work to emergence of resilience in socio-technical systems.

2. METHODS

The goal of our work is to provide a framework that supports the execution of experiments in the spirit of concept development and experimentation (CD&E). With the intention to get there, we will use the term resilience rather as a technical term than as general concept. We put our focus on drawing the margins of the framework tightly around the core of the resilience concept, leaving everything aside that might be covered by other related concepts as robustness, resistance or sustainability. Furthermore, we will take a performance driven perspective on resilience covering aspects as safety and organizational performance.

To begin with, we need an operationalizable definition of resilience. In favor to get there, we will refer to resilience as a property of systems only to emerge in a state of overload. Overload occurs, as soon as performance requirements (R) exceed the response capabilities (C) of a given socio-technical system. Therefore, overload can be formalized as $C/R<1$. Continuing from this definition we suggest a resilience framework consisting of four elements: 1) phases; 2) principles; 3) capabilities and 4) mechanisms.

2.1. Phases

Resilience emerges dynamically as the system is entering the state of overload. In response to this evolution the system may experience timely separated phases.

2.2. Principles

Principles are strategies to be followed to enable the emergence of a resilient reaction when the system is entering a state of overload. The principles require specific abilities to generate this response.

2.3. Capabilities

Capabilities emerge from successful application of a single mechanism or a set of specific mechanisms.

2.4. Mechanisms

Mechanisms are the means by which actions and reactions can be carried out. Mechanisms are based on tangible, intangible as well as human resources, such as specific tools or rules for example.

3. RESULTS

As stated before, we regard resilience as an emergent property of a system under strain and not as a capability by itself. As requirements exceed a systems nominal performance, it starts to mobilize all available resources and reserves to withstand the strain mobilizing maximum performance. If maximum performance exceeds a critical time frame or requirements further increase, the system enters the state of overload and resilience may emerge in a dynamic response of the system to the strain it is exposed to. This reaction evolves in two phases, the degradation and the adaptation phase. Based on successful adaptation, new system capabilities are developed and implemented until system capabilities exceed the situation requirements ($C_{New}/R>1$) and the system completes the resilience cycle by returning to normal operation.

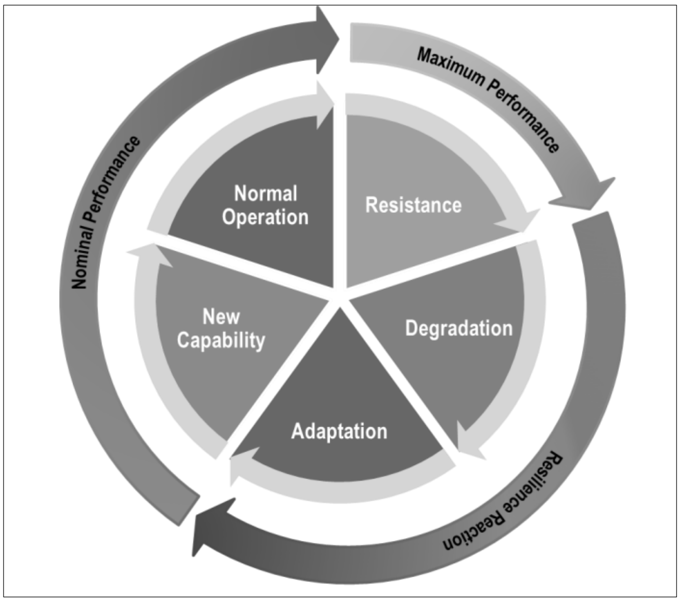


Figure 2. *Resilience cycle*

3.1. Degradation Phase

As the maximum performance of a system is exceeded it starts to degrade over time as overstressed parts and functions fail and losses occur. To be able to degrade, three principles proved to be important. These are the principles of 1A) autonomy, 1B) fractality and 1C) compatibility.

The *1A) principle of autonomy* refers to the locus of control, which must stay with the acting and deciding entities to enable timely and (hierarchy-)independent decisions based on the knowledge and experience of the involved entities. This will foster the use of local intelligence as an important prerequisite for the capability of self-synchronization to evolve.

The *1B) principle of fractality* enables organizational stability during the degradation of the system, when teams and units are constantly breaking up and reconfiguring to keep up a functional organization, hence producing a scalable organization. A functional organization is crucial to keep up a significant system output in the state of degradation [Danner-Schroeder & Geiger, 2016].

The *1C) principle of compatibility* enables the recombination of system parts in a different way than they were designed for. Hence, such parts can be used as replacement for failing but crucial other system parts and the system may serve as its own spare parts stock. This is true for organizational structures as well as for infrastructure, hard-, soft- or liveware.

3.2. Adaptation Phase

The degradation phase blends over into the adaptation phase and vice versa. This means that there is a constant overlap of the two phases at any given time during a resilience reaction, but the ratio significantly changes over time in a directed manner. Three principles are crucial to enable adaptation. These are the principles of 2A) diversity, 2B) selection and 2C) standardization.

The *2A) principle of diversity* is addressing the fact, that adaptation depends up on a minimal level of variance in the system. Either, there is a sufficient level of diversity already in the system or it should be created by introducing variance into the system, for example by accepting deviations from rules and SOPs and by letting people solve problems by trial-and-error tactics. At this point, one important thing to keep in mind is to carefully control the level of variance introduced into the system to avoid that the system is shifting to a chaotic state. Hence, if variance is introduced into a system it should happen in a controlled manor.

Once promising solutions to problems have been found, *2B) selection* starts and the solutions are undergoing a testing phase. As soon as a workable solution is selected, it is going to be implemented in the system.

The *2C) principle of standardization* is addressing the process of implementing a new capability or problem solution into an organization. So, standardization is a manifestation of learning in an organization, ensuring the system-wide application of the new capabilities and their application in the most effective and efficient way.

3.3. Capabilities & Mechanisms

As stated above, capabilities emerge from successful application of a single mechanism or a set of specific mechanisms. So, if we are going to assess a system regarding its resilience potential, it all comes down to the identification and evaluation of the resilience enabling mechanisms present in the system. The mechanisms might vary between different organizations. Some of them might have a more universal and generic character such that they reappear constantly in resilient systems albeit in changing appearance. Examples for this could be generic rule-sets, role-based organization, modularity, standardization, improvisation or selection by trial-and-error tactics.

Table 7. *Element-structure of the resilience framework*

Phase	Principle	Capability	Mechanism (examples)
Degradation Phase	1A) Autonomy	- Timely Decision Making - Use of Local Intelligence	- Involved and Acting Entities Decide for Themselves
	1B) Fractality	- Self-synchronization - Scalable Organization	- Generic Rules - Role-Based Organization
	1C) Compatibility	- Recombinability	- Modularity - Standardization
Adaptation Phase	2A) Diversity	- Creativity	- T-Shapes (Polyvalence) - Improvisation
	2B) Selection	- Testing	- Trial & Error
	2C) Standardization	- Learning & Implementation	- Adaptive SOP

4. CONCLUSIONS

When planning for a resilience experiment, we may follow the guidance provided by the definition of resilience and the four elements of the resilience listed in the framework. First, we would probably like to check for the presence of resilience. As discussed above, resilience is a system property to emerge in an overloaded system. Hence, if the condition C/R<1 is not met, we are not looking at resilience. Second, we may specifically check for the presence of core principles, capabilities and mechanisms. Third, we could also want to look at the system performance. In some particular cases, we might detect a typical resilience performance curve, as an exemplary expression of resilience. This will most probably be the case in a situation, where a timely limited disturbance, like a shock, occurs. This could typically be the case after an isolated event like an earthquake, flooding or power failure for example. It will be less probable, if the disturbance persists or even progresses over time as it would be the case in a war situation for example.

Acknowledgements

The work reported in this paper was supported by the Swiss Procurement Agency armasuisse.

REFERENCES

Meredith, L. S., Sherbourne, C. D., Gaillot, S., Hansell, L., Ritschard, H. V. Parker, A. M. & Wrenn, G. (2011). Promoting Psychological Resilience in the U.S. Military, RAND Corporation, www.rand.org/content/dam/rand/pubs/monographs/2011/RAND_MG996.pdf

Kutsch, E., Hall, M. & Turner, N (2015). Project Resilience, Gower Pub. Ltd., Farnham, UK. ASIS SPC.1-2009 Standard (2009). Organizational Resilience: Security, Preparedness and Continuity Management Systems—Requirements with Guidance for Use.

Pflanz, M. & Levis, A. (2012). An Approach to Evaluating Resilience in Command and Control Architectures, Conference on Systemsengineering Research (CSER), 2012, St. Louis, MO, USA.

Kim, Y., Chen, Y.-S., Linderman, K (2015). Supply Network Disruption and Resilience: A Network Structural Perspective, Journal of Operations Management, Vol. 33-34, p. 43-59.

Homeland Security (2014). The 2014 Quadrennial Homeland Security Review, https://www.dhs.gov/publication/2014-quadrennial-homeland-security-review-qhsr. United Nations (2017). United Nations Plan of Action on Disaster Risk Reduction for Resilience, http://www.preventionweb.net/publications/view/49076.

Freitas, A. L. & Downey, G. (1998). International Journal Of Behavioral Development, Vol. 22, No. 2, p. 263-285.

Ayling, J. (2010). Criminal Organizations and Resilience, International Journal of Law, Crime and Justice, Vol. 37 p. 182-196, www.elsevier.com/locate/ijlcj.

Välikangas,L (2010). The Resilient Organization -How Adaptive Cultures Thrive Even When Strategy Fails, McGraw Hill Comp., USA.

Walker, B. & Salt, D. (2006). Resilience Thinking – Sustaining Ecosystems and People in a Changing World, Island Press, Washington DC,USA.

Gallopin, G.C. (2006). Linkages between vulnerability, resilience, and adaptive capacity. *Global Environmental Change 16* (pp. 293–303). Elsevier Ltd. www.elsevier.com/locate/gloenvcha

Prior, T. & Herzog, M (2013). Risk Factsheet 9. The Practical Application of Resilience: Resilience Manifestation and Expression. *3RG REPORT, Risk and Resilience Research Group, Center for Security Studies (CSS).* ETH Zürich.

Gibson, C. A. & Tarrant, M. (2010). A 'conceptual models' approach to organisational resilience, The Australian Journal of Emergency Management Vol. 25, No. 02.

Militello, L. G., Branlat,M., Lopez, C. E., Walker, K. E., Finomore, V., Ritter, J., Bean, R. & McGraw, D. (2013). Decision Support for Pararescue, International Conference on Naturalistic Decision Making, Marseille, France.

Danner-Schroeder, A. & Geiger, D. (2016). Organsationale Resilienz: Wie Unternehmen Krisen erfolgreich bewältigen können. *Zeitschrift Führung und Organisation* (pp. 201-2018). Stuttgart: Schäfer-Poeschel Verlag für Wirtschaft, Steuern, Recht GmbH.

SERIOUS GAMES: AN EFFICIENT TOOL FOR THE LEARNING ABOUT CITY RESILIENCE

Iturriza, M., Labaka, L. and Sarriegi, J.M.
Tecnun Universidad de Navarra, Paseo Manuel Lardizabal 13, Donostia, Spain
miturriza@tecnun.es

Abstract

Natural and man-made disasters are becoming more frequent lately and as a consequence, the relevance of resilience has increased significantly over the last years. Hence, there is a need for building city resilience yet there is a lack of guidance about what policies and steps should be followed in order to resist, absorb, adapt and recover from a crisis. In this context, Smart Mature Resilience (SMR) project, funded by the Horizon-2020 program, wants to develop a guideline for cities to improve their resilience level. The SMR project defines a Resilience Maturity Model (RMM) to determine the optimum path towards building the city resilience. In addition, the project develops a Serious Game (SG), aiming at presenting the RMM based on a system dynamics model that is encapsulated in a user interface. However, the benefit of using SG for didactical applications is not always clear, as there are examples that failed their purpose. Therefore, this paper presents the requirements the serious game should fulfil, explains the practical case of the pilot version developed in the SMR project and discusses how the pilot version achieves the established requirements.

1. INTRODUCTION

Cities continue to grow and as a consequence there is a need to build city resilience, not only theoretically but also in a more practical way. There are several researches that define resilience policies and actions in order to achieve higher resilience levels (Gimenez, Hernantes, & Labaka, 2016). However, none of these studies explain the inter-relations existing between the policies and their operationalization.

Therefore, recent crisis and catastrophic events have led to an increase of awareness regarding the necessity of developing tools which facilitate decision makers and crisis managers to deal with crisis and become more resilient. Decision makers such as local governments or involved stakeholders demand tools which enable to train and learn from past experiences in order to get prepared for future disasters. As a consequence, the use of serious games (SG) for didactical uses has augmented lately. Society has evolved into a more interactive and practical society (Kiili, 2005; Mayer et al., 2014) and, therefore, the way knowledge is taught and interiorized by learners has changed (Guillén-Nieto & Aleson-Carbonell, 2012). In some cases the literature shows that the use of SG have failed their purpose whereas in other cases it shows the high benefits of using SG for didactical application (Vogel, Bornhovd, Neupert, & AS, 2006).

This paper presents the practical case of a SG developed in the Smart Mature Resilience (SMR) European project, which aims to provide a tool for decision makers to train themselves. The SG presented in this paper is a pilot version of the one developed for the SMR project and therefore the complexity of the design is simplified yet the main characteristics are maintained. First, in Section 2, the context and necessities the decision makers have are pointed out followed by the description of the SMR tool (Section 3). Then, in Section 4, how the SG copes with the requirements is discussed and finally, in Section 5 the conclusions are made.

2. STATEMENT OF THE PROBLEM

The number of disasters has increased in the last decade with twice as many disasters and catastrophes than in the last decade of the 20th century. This, in turn, has augmented the awareness to improve the ability to manage and assess the cities' resilience. However, how to manage with already known risks and get prepared for unexpected ones is a complex activity as crisis management is unpredictable and it is not possible to know when disasters will occur and which the consequences will be (Coleman, 2004). In order to cope with this necessity a SG has been developed with the aim of providing decision makers with a tool to train, experiment and understand real life scenarios.

However, even if a SG is a tool which enables decision makers to better understand the concerning problem, to take more appropriate decisions and get to know the system under study there is not a consensus in the benefits and success of using them. In some cases the objectives when applying SG for interactive learning have not been achieved (Erhel & Jamet, 2013). The main cause for not developing a successful SG application is not having a clear goal during the design process (Greitzer, Kuchar, & Huston, 2007).

As a consequence, before developing the SG, the requirements the SG should have were pointed, taking into account the final user will be decision makers such as governments or involved stakeholders:

1. Training tool: Decision makers need to be able to train themselves with tools which represent real life scenarios in order to get prepared to face future disasters. To do so the SG should represent the reality and fulfil the following three characteristics:
   a. Holistic perspective: Users might be specialized in specific topics and might not be aware of other realities. Therefore, the SG should provide and encourage a holistic perspective that ends with the silo mentality users might have. This way, the decision makers who use the SG should end up with a broad perspective of crisis management not only being aware of their specific area but also understanding other sectors.
   b. Temporal order between policies: The policies chosen to get prepared and face a disaster do not have to be implemented at the same time but they should be applied in a specific order, since they are interrelated. However, decision makers might not know that the policies should be implemented following a temporal order in order to be more efficient. As a consequence, the SG should provide the user the opportunity to learn about which is the most efficient path to implement these policies.
   c. Relationships between policies: Decision makers use the SG in order to better understand how the policies are interrelated with each other and their effect. Therefore, the SG should interactively represent the existing temporal and interdisciplinary relationships between policies, as well as the impact of implementing the policies not taking into account these relationships.
2. Trustworthy: The SG should represent a city and show trustworthy results in order to provide decision makers a tool to study the impact of the implemented policies. Therefore, the SG should be parametrized with real cities' data with the objective of showing credible consequences after implementing a policy. As a consequence, the SG will make the decision makers aware of the counterintuitive consequences a decision could have.
3. Flexible: Disasters often happen unexpectedly and the context in which they could happen can be diverse. As a consequence, the SG should be flexible, enabling decision makers to adapt the game to different situations and contexts such as socio cultural aspects, economic structures or different types of critical infrastructures, as well as enable to choose the type of disasters the SG will simulate.

3. SMR'S TOOL: A PRACTICAL CASE

Smart Mature Resilience (SMR) is a European project funded by European Union's Horizon 2020 (H2020-EU.3.7., project ref. 653569) which develops a resilience management guideline based on a Resilience Maturity Model (RMM) that engages a growing number of stakeholders and multi-level governance in order for cities to become more resilient. In this context, the SMR project develops a tool; a SG which embodies the key aspects of the RMM.

3.1 Game description

The SMR's SG aims to develop a reflexive SG which assists decision makers to understand the structure of the RMM in order to enable doing experiments to study policies before implementing them in the real life. The RMM defines the path towards cities need to go through in order to improve their resilience level. It is composed of policies which are classified based on four resilience dimensions (Leadership & Governance, Preparedness, Critical Infrastructures and Cooperation) and five maturity stages (Starting, Moderate, Advanced, Robust, Vertebrate). Through the implementation of the policies, cities achieve higher maturity stages in a systematic and incremental way. The resilience policies defined in the RMM are inter-related and therefore, some policies are predecessors of others. Thus, depending on the order in which policies are applied, the efficiency of the implemented policies will vary and consequently the progress in the maturity stage will depend on that. Therefore, the SG targets to make aware decision makers about the policies' interrelationships, their dynamic behavior and the possible unintended consequences that may arise due to these precedence relationships.
Concerning its structure and design, the SG is composed of a System Dynamics model (SD), which defines the logic and the structure of the model based on the RMM and a user friendly interface that interacts with the user in order to obtain the input data and show the results. The SG can be used by any person, however it is oriented to be used by cities, specifically to by people who work on strategic levels with a holistic perspective and building

resilience. Moreover, the SG is general and cannot be particularized to disasters. The results showed in the game represent a city of 800.000 inhabitants which would be similar to Amsterdam and a GDP of 35.500 similar to the city of Rome. This values are obtained after parameterizing the information and characteristics of the cities participating in the project (*Bristol*, *Rome*, *Riga*, *Glasgow*, *Vejle*, *Kristiansand* and *Donostia*).

Regarding the functionality of the game, the input of the SG are the policies defined in the RMM. During the game the user chooses the policy implementation order and how much to investment on each. As a consequence, the SG shows the impact of the taken decisions through time evolution graphs and indicators.

The SG is structured in three screens; initial state screen, decision-screen and result-screen. When the users enter the tool they go into the initial state screen where the purpose and functionalities of the game are briefly defined. In this screen the users need to choose the current maturity stage and the annual available budget (see figure1). Although the annual available budget is predefined, the budget can be changed at any moment in any of the three screens.

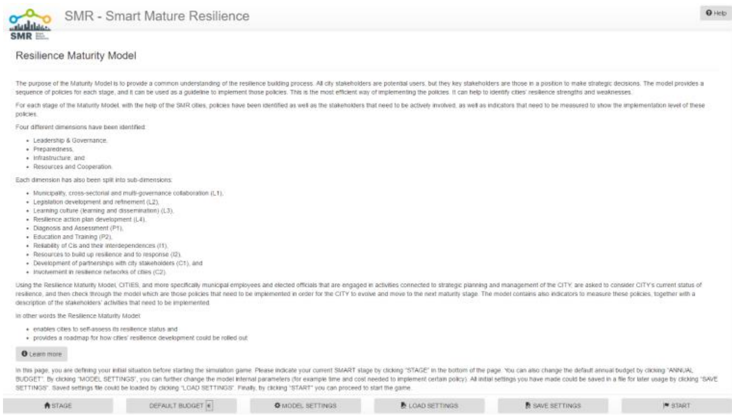


Figure 4 *Initial state screen*

Once the initial situation is established, the users move to the decision screen. In this screen, the users select how much money they allocate to each policy. The screen shows the list of resilience policies already defined in the RMM, classified by the four Resilience dimensions and five maturity stages (see figure2). Moreover, a short explanation of each policy appears when the mouse is put over the policy. Using the "Advance 1 year" button, the game simulates for one year, spending the available annual budget on the selected policies.

Apart from that, the indicators related to the current year of the game, the available annual budget and the budget left are showed as well as the buttons to change the available annual budget, to start a new game called "New scenario" and to go to result-screen called "Simulation results".

Figure 5 *Decision screen*

The result-screen shows the results of the simulation based on the taken decision (see figure3). At the top left hand of the screen the percentages of the current implementation, named "Actual", and the efficiency of the implementation of the policies, named "Effectiveness", are presented for each resilience dimension. The

"Actual" percentage represents the implementation level of the policy and "Effectiveness" percentage represents the effectiveness of the implementation. These two percentages aim to represent the consequences of the relations existing between the policies. Therefore, if policies are not implemented in the correct order percentages will show low effectivity and implementation in comparison of what the user has decided in the decision-screen. Below this table, the speedometers are used to indicate the maturity stage the user has achieved in each resilience dimension. The speedometers start at 0 and go from the starting stage to vertebrate passing through moderate, advance and robust (S, M, A, R, T). Moreover, at the top right hand of the screen resilience dimension's implementation level results are presented through time evolution graphs. The simulation ends at 40 years, therefore time cannot be greater than 40 and the level of implementation is complete when the 100% is achieved.

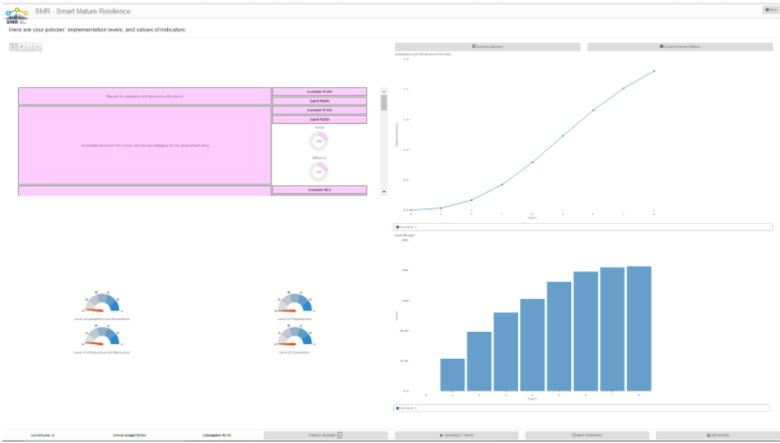


Figure 6 *Result screen*

Bellow the graph the evolution of the used total budget is represented through a time evolution graph where the time is represented in years and the budget in Euros. Furthermore, on the bottom of the screen the current simulation year, the available annual budget, the left budget and the button that gives the possibility to change the annual budget are shown. Furthermore, the buttons to step forward one year, to begin a new scenario and to go back to the decisions-screen are also represented.

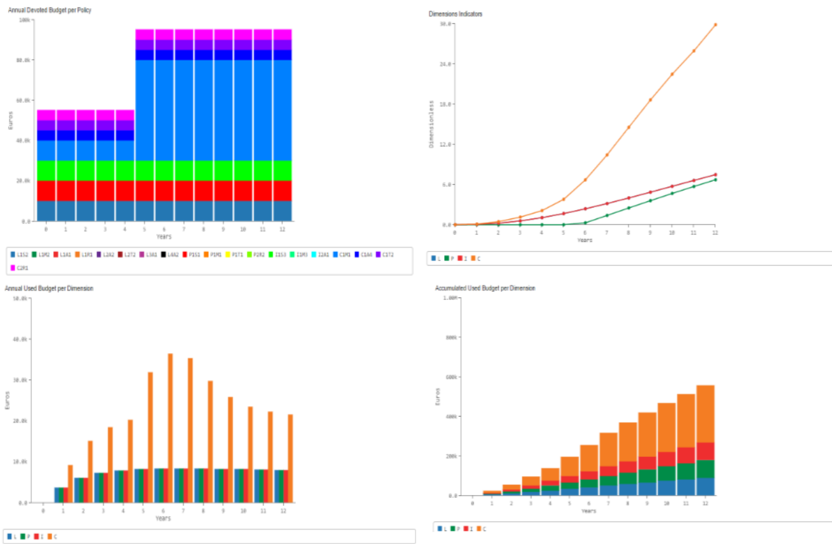


Figure 7 *Current scenario details graphs*

Apart from that, when clicking on the top right button called "Current scenario details" more detailed information concerning how the budget has been invested can be found (see figure4). In this additional result-screen, graphs regarding the level of implementation of the policies and the evolution of the spent budget are shown. The graph representing the implementation level resumes how the resilience dimensions have evolved over time per dimension. Below, the graphs concerning budget represent the accumulated budget per resilience dimension, annual devoted budget per policy and annual devoted budget per resilience dimension.

4. RESULT

Following, how the defined 6 requirements defined in Section 2 have been fulfilled in the SMR's SG is explained. In particular, the different functionalities that have been included in the tool in order to fulfill these requirements are explained.

1. Training tool: The developed SG enables the decision makers to try different policy implementation options and study their impact through indicators and graphs. Therefore, the SG provide decision makers a tool to train themselves.

    a. Holistic perspective: The SG developed in the SMR project encompasses the policies defined in the four resilience dimensions defined in the RMM. Therefore, all the fields (Leaderships and Governance, Preparedness, Critical Infrastructures and Cooperation) are represented. This means that the user who is playing with the SG should have a holistic view of the problem and not just a view of its particular area. Apart from that, there is no limitation regarding the user, any person from any particular area, specialization or background could use it. As a consequence, the SG enables the user to make aware that the decisions taken could influence not only in one resilience dimension but also in others. To do so, the SG shows how the resilience dimensions evolve over time and which is the direct effect of the taken decisions.

    b. Temporal order between policies: The SG is composed by different indicators and time evolution graphs that aim to make the user aware of the impact of the taken decisions. In order to make them realize how the implementation order affects, percentages per policy named "Actual" and "Effectiveness" have been used. The objective of these percentages is to show visually the importance in the implementation order as the decisions taken in the SG have to be what happens in reality.

    c. Relationships between policies: The developed SG is based on the RMM and it takes into account the precedence linear and transversal relationships between the policies. Therefore, in order to make the decision maker aware of these precedence relationships, every four years of simulation, the SG shows pop-up messages to the user explaining the errors he has committed. As a consequence, the SG enables the user to learn which are the relationships existing between policies and therefore the optimum path towards resilience.

2. Trustworthy: The SG have been parametrized through a workshop in which 7 European cities have participated. Therefore, the showed results represent the impact of the taken decisions in all the resilience dimensions for a standard city. The resulting graphs indicate the level of implementation of the policies whereas the speedometer indicators indicate the maturity stage of each resilience dimension. Thus, decision makers will obtain trustworthy results which ensure the conclusions they get will help them achieving their resilience objective.
3. Flexible: The designed SG can be considered flexible due to several reasons. On the one hand, it is possible to stablish the initial maturity stage level aiming to represent different situations cities might be in. On the other hand, the SG enables to change the available budget during the game in order to be able to represent budget cuts or budget reductions. Apart from that, it is possible to adjust the critical parameters that define the characteristics of the represented city. This way parameters such as implementation cost or time for implementation can be adapted as they depend on the cities characteristics. Moreover, the SG enables to save and share the obtained results, therefore, it provides the opportunity to learn of other users' experience. However, the actual SG is not prepared to be particularized to specific disasters. Thus, next steps could be to develop an updated version which allows to particularize the disaster under study.

5. CONCLUSION

Recent natural and man-made disasters have led to the increase of awareness regarding the necessity of developing the resilience of cities. However, building resilience is a complex activity as disasters and crisis are unpredictable and difficult to manage. In order to reduce this complexity, recent studies have developed resilience frameworks, policies and actions which enable to achieve higher resilience levels.

In parallel, the use of SG has been a recent topic lately. SG have shown high benefits when applied for didactical objectives to better explain complex problems. However, a SG should accomplish some stablished requirements in order to ensure its success.

In this context, SMR European H2020 project develops a RMM which defines resilience policies that cities should implement in order to build their resilience level. In order to better explain the RMM and get a higher impact, a SG has been developed. The SG is based on the RMM and encapsulated in a system dynamics model and a user friendly interface. The game is divided into three screens: initial state screen, decision-screen and result-screen. This paper discusses how the preliminary version of the SG developed in SMR fulfils the established requirements. As a conclusion, it can be said that all the requirements have been fulfilled and that as a future step the SG could allow the user to particularize the game to its specific situation and disaster problem.

6. REFERENCES

Coleman, L. (2004). The frequency and cost of corporate crises. *Journal of Contingencies and Crisis Management*, *12*(1), 2–13. https://doi.org/10.1111/j.0966-0879.2004.01201002.x

Erhel, S., & Jamet, E. (2013). Digital game-based learning: Impact of instructions and feedback on motivation and learning effectiveness. *Computers and Education*, *67*, 156–167. https://doi.org/10.1016/j.compedu.2013.02.019

Gimenez, R., Hernantes, J., & Labaka, L. (2016). Technological Forecasting & Social Change A maturity model for the involvement of stakeholders in the city resilience building process. *Technological Forecasting & Social Change*. https://doi.org/10.1016/j.techfore.2016.08.001

Greitzer, F. L., Kuchar, O. A., & Huston, K. (2007). Cognitive science implications for enhancing training effectiveness in a serious gaming context. *Journal on Educational Resources in Computing*, *7*(3), 2–11. https://doi.org/10.1145/1281320.1281322

Guillén-Nieto, V., & Aleson-Carbonell, M. (2012). Serious games and learning effectiveness: The case of It's a Deal! *Computers & Education*, *58*(1), 435–448. https://doi.org/10.1016/j.compedu.2011.07.015

Kiili, K. (2005). Digital game-based learning: Towards an experiential gaming model. *Internet and Higher Education*, *8*(1), 13–24. https://doi.org/10.1016/j.iheduc.2004.12.001

Mayer, I., Bekebrede, G., Harteveld, C., Warmelink, H., Zhou, Q., Van Ruijven, T., … Wenzler, I. (2014). The research and evaluation of serious games: Toward a comprehensive methodology. *British Journal of Educational Technology*, *45*(3), 502–527. https://doi.org/10.1111/bjet.12067

Vogel, F., Bornhovd, C., Neupert, W., & AS, R. (2006). Dynamic subcompartmentalization of the mitochondrial inner membrane. *The Journal of Cell Biology*, *175*(2), 237–247.

USING SIMULATION GAMES TO ASSESS CRITICAL INFRASTRUCTURE RESILIENCE IN CASE OF PAYMENT DISRUPTIONS

Björn JE Johansson [1], Joeri van Laere [2], and Peter Berggren [3]

[1] Linköping University, Sweden

[1] bjorn.j.johansson@liu.se

[2] University of Skövde, Sweden

[2] joeri.van.laere@his.se

[3] Linköping University, Sweden hyperlink

[3] peter.berggren@liu.se

Abstract

This paper presents a theoretical outline, and a tentative assessment approach, for resilience in the fuel, food, and finance systems needed to create a gaming simulation environment. The purpose of developing the simulation gaming environment is to provide team-training to decision-makers in handling crisis situations in a multi-organisational context. Gaming simulation aims at representing reality and enabling an individual actor or a group of actors to experience the dynamics of the simulated system. The concept of core values and resilience value networks will be used to guide the simulation approach so that all core functions of a resilient system, as well as coping strategies, will be addressed in the gaming sessions.

INTRODUCTION

Infrastructures for fuel, food and payment systems become increasingly entangled (Ansell, Boin, & Keller, 2010) by being dependent on each other and on a large variety of support systems as well as other systems that provide services crucial for the function of the overall system. When a disturbance occurs, the resilience of these infrastructures depends on the ability to produce collaborative responses from individuals with diverse backgrounds that may not be familiar with side impacts in totally different areas. This is a challenging task in a complex environment such as the fuel, food and payment systems, and preparation in terms of training and development of strategies is crucial for the management of disruptions.

This paper presents the outline for a project (Creating Collaborative Resilience Awareness, Analysis and Action for Finance, Food and Fuel Systems in INteractive Games, CCRAAAFFFTING) aiming to develop a simulation gaming (a combination of role-playing games and computer simulation) that can be used to better understand how resilience is achieved and maintained during disruptions in the payment, food, fuel and finance system. The ultimate purpose of developing the gaming environment is to provide team-training to decision-makers in handling crisis situations in a multi-organisational context. Gaming-simulation (Laere, Vreede & Sol, 2006) aims at representing reality and enabling an individual actor or a group of actors to experience the dynamics of the simulated system. Given the variety of interpretations of resilience (Bergström, van Winsen & Henriqsen, 2015), resilience is hard to operationalize into useful strategies and measurable indicators. Lundberg and Johansson (2015) have therefore proposed the Systemic Resilience Model (SyRes) model as a way to describe process, functions and strategies on a conceptual level in an effort to synthesize different perspectives in the field of resilience research. The SyRes-model will be used to guide the simulation approach so that all core functions of a resilient system, as well as coping strategies, will be addressed in the gaming sessions. The project started in 2016 and initial data collections based on document studies, interviews and workshops with experts from the food, fuel and financial sectors reveal seven challenges for collective cross-functional critical infrastructure resilience that need to be dealt with: 1) Shortage of food, fuel, cash, medicine; 2) Limited capacity of alternative payment solutions; 3) Cities are more vulnerable than the countryside; 4) Economically vulnerable groups in society are more severely affected; 5) Need to maintain trust and prevent panic; 6) Crisis communication needs; 7) Fragmentation of responsibility for critical infrastructures across many actors (Laere et al, 2017). This paper presents the theoretical outline for understanding resilience in the fuel, food, and financial systems needed to create the gaming simulation environment, as well as an assessment approach for evaluating resilience in the gaming sessions.

UNDERSTANDING RESILIENCE IN CRITICAL INFRASTRUCTURE

“Resilience” as a term is certainly in vogue, and most any business, governmental agency or public actor has joined the chorus of aiming to become more resilient. However, the term is often used in a general fashion, without stating in what way something (a "system") should be resilient. Both Lundberg and Johansson (2015) and Bergström, van Winsen and Henriqson (2015) list that resilience amongst others can refer to: bouncing back to a previous state, or bouncing forward to a new state, or both; absorbing variety and preserve functioning, or recovering from damage, or both; and being proactive and anticipating, or being reactive (when recovering during and after events), or both. This is not surprising as the term largely emerged as a consequence of the realization that not all disturbances or threats towards a system can be predicted. Hence, safeguarding known or foreseeable threats will never be sufficient for coping with events that an increasingly complex environment potentially can throw at you. This has been discussed thoroughly in for example Hollnagel's description of Safety I vs Safety II (Hollnagel, 2013). Further, the term has been defined and re-defined so many times that it almost has become diluted, causing confusion and uncertainty regarding what actually is meant by resilience and what being resilient comprise.

Lundberg and Johansson (2015) made an effort to merge and compile different points of view in the field of disaster and crisis response resilience into one systemic model, the *Systemic Resilience Model* (SyRes). The model departs from the idea that the coping with an unwanted event can be seen as a downward spiral activating certain basic resilience functions (anticipation, monitoring, responding, recovery and learning) and their associated strategies (where the strategies are the actual manifestation of the functions, or their 'form', which may differ from system to system). Further, Lundberg and Johansson (2015) suggest that resilience is needed to protect *core values*, i.e. values central for the existence of the system in focus, or their "rational". In safety-critical systems, such core values usually take the form of maintaining safety, such as avoiding harm to humans or critical infrastructures. For a commercial business such as a grocery store, a petrol station or a bank, a core value is typical to create revenue, i.e. to assure a higher income than outcome. Without this profit, the business will seize to exist. This core value will manifest itself in a number of practical activities which usually take the form of different flows such as goods, money, services etc.

If we accept that all threats cannot be foreseen, and hence coped with by creating barriers, procedures and protection systems, then being resilient must be about what a system need to protect and preserve, its core values, instead of what threats it should be able to cope with. How to "invest" in resilience will therefore be a question about understanding what these core values are and in what way flexible approaches to protecting and upholding these values can be created. According to the SyRes-model, basic resilience functions such as anticipation, monitoring, response, recover and learning, with their associated strategies (the manifestation of the functions) can be coupled to each core value as a means for resilience. Naturally, the nature of the core value will impact in what way the function becomes manifest in terms of strategies, as well as what type of strategies are meaningful in relation to the specific core value. Also, the possibility that harm can come to the system and its values must be acknowledged. Investing in detecting and coping with potential threats is thus not enough. The system must be able to maintain core values also when situations occur that disrupt existing functions. For example, a business must be able to continue generating revenue even when payment systems fail, or at least assure that existing assets are not depleted and that readiness exists for rapid re-establishment of payment processes. As the reader probably already understands, this implies a set of core values for each system of interest, a *core value ladder*.

Asking a business owner what his or her core values are will probably render a number of answers ranging from the well-fare of employees, customer satisfaction, sustainable business plans, shareholder benefits and so forth. However, historical financial crisis situations have shown a surprising versatility when it comes to re-arranging businesses with the ultimate survival (on the market) as the primary objective. Firing large proportions of the workforce, moving business units to other countries, merging with similar firms, or simply selling of large proportions of the business are all well-known strategies for coping with unfavourable conditions. A disruption in the payment system may, at least for a small business, be at least as devastating for a smaller business as a financial crisis, especially if it occurs during an expected peak in sales. However, businesses, like most open systems, do not exist in a vacuum. Instead, the very pre-conditions for their existence are the exchange of flows with other systems (for the sake of the argument, we will henceforth describe each business as a "node" in the larger financial system).

Basole and Rouse (2008) looks at how "service value" can be created in a network context and how the structure and dynamics of the network, as well as customer expectations influence the complexity of the service eco system. Their approach aims to describe the nature, delivery and exchange of service value and direct and indirect relationships between value network actors. In a similar fashion, value networks can be used for understanding how networks of actors can create and consume resilience in a network. In the model of Basoule and Rouse (2008), consumers (although forming their own networks) are always the ones that realize value, as provides of service have no real purpose unless there is a consumer. In the case of resilience, there are differences regarding what "value" is and how it is exchanged between different actors. For example, in a situation where the credit card terminal fails, alternative payment solutions may be invented by customers, effectively rendering the customers the source of resilience rather than the business in itself. It should also be noted that while service value networks also have a degree of dynamics in terms of how relations between nodes emerge and disappears, a resilience value network often has to be initiated rapidly in a time of dire need, suggesting that the actual structure of the network may be hard to predict. Further, as core values of individual nodes may change in a crisis situation (according to the value ladders of each node), the *resilience value network* may also change (see Figure 1).

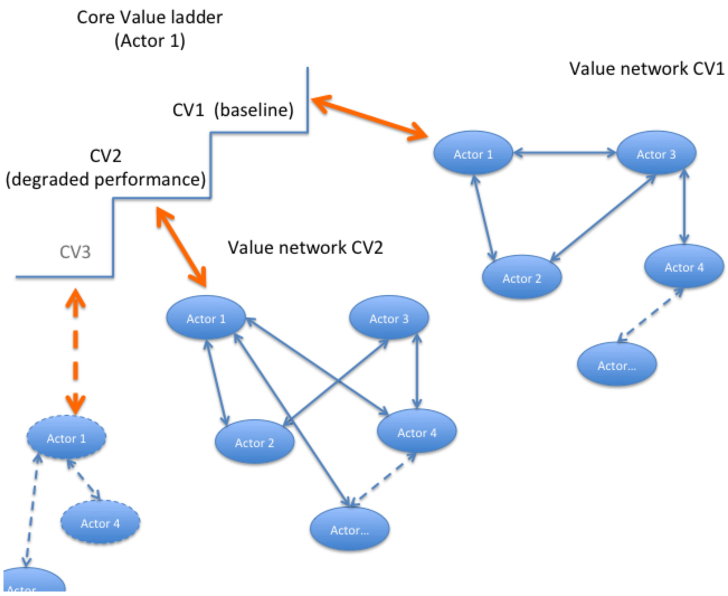


Figure 1. The core value ladder of an individual node in the resilience value network can potentially cause changes to the network if a node moves from one step on the core value ladder to another

Likewise, if the supplier flow of goods is interrupted for some reason, stores may be able to temporarily counter-act this by moving goods between themselves. This will help sustaining revenue, but the strategy will only provide resilience as long as there are collective resources in the network to pull from.

A basic condition for understanding the resilience value network is to understand how collaboration works, as collaboration allows for resilience "pooling". During a crisis event, stakeholders need to come together and seek solutions to problems. In the case of disturbances in the financial system, actors that do not normally cooperate may have to work together to create processes that help them uphold core values in their respective systems. Collaboration, in turn, is based on trust, the willingness to exchange information and the ability to take on roles that are responsible for specific aspects of problem solving. In practice, co-located actors need to form one or more teams that jointly try to cope with the problem at hand.

GAMING SIMULATION

A possible way of both investigating and improving system performance could be to challenge one or several actor(s) core values in a sufficiently detailed simulation. By adapting a learning-by-experience-based approach, stakeholders can be presented with challenging situations in a safe environment where they can test different approaches to coping with unusual or even unexampled events (Wachs et al., 2016). Such a simulation can take many forms, from tabletop exercises to full-scale exercises involving multiple actors. The latter approach can provide many opportunities for identifying how a resilience value network develops between different actors, but it is also a challenge as it may be difficult to capture and understand interactions between the involved entities. Indeed, it may be demanding and costly to create such a simulation as it can require involvement of very many actors, a large and cumbersome simulation management and a multitude of expert analysts in order to evaluate what actually took place and what it means. On the other hand, synthetic task environments "…can facilitate research in a safe and inexpensive setting and can also be used for task training and system design in support of tasks" (Cooke & Shope, 2004, p. 264). Caluwe et al (2012) and Daalen et al (2014) discuss extensively how simulation games successfully have been used to study the interaction between stakeholder decisions in complex design problems. Simulation-games can be used for exploring the feasibility of future policy alternatives, for studying and motivating organizational change, and as research tools to study the processes or organizational change, policy-making and stekaholder interaction.

Scenarios that are intended to be used for improving resilience must present events that *challenge the participating actors in such a way that they are forced to engage in collaborative problem-solving*. In typical training or exercise scenarios, participants are encouraged to apply known procedures or skill sets. This would not be the case when training to become more resilient. Rather, the capacity of the involved organizations needs to be challenged in situations that have not been prepared in advance. Preferably, *the scenario should demand information exchange with other actors or entities that they do not normally interact with as a way of challenging (and invoking) the resilience value network*. Creating events within the scenario that challenge these aspects is thus a core task for the scenario designer. Rome et al. (2016) models resilience in a gaming-simulation by distinguishing the impact of mitigating actions. For example, when citizens in case of a flooding either are informed to take preventive measures or evacuated in time, less damages and injuries/fatalities occur. Players can go back to earlier moments in the simulation and in that way explore alternative action paths and see the difference in consequences of their different mitigation strategies. Kurapati et al (2015) take a different approach and model resilience as balancing actions that serve individual department score versus the organizational score (the common interest of all departments). When the players collaborate (share information with the right departments, choose actions that serve the common interest) the overall organizational score benefits, and the organization is seen as more resilient.

ASSESSMENT

When doing any type experiments or evaluations of human (or system) performance, it is always challenging to identify appropriate performance measures. When assessing resilient performance, this is possibly even more challenging as there are few descriptions of what successful resilience *is*, how it manifests itself in terms of strategies and behaviours, apart from what can be found in different definitions such as to "recognize and adapt to handle unanticipated perturbations" (Woods, chapter 2 in Hollnagel, Woods & Leveson, 2006). A well-known paradox in all safety related activities is that what can be assessed before a critical event always has to be the potential for safety or resilience as it by definition is impossible to say if implemented measures are going to make a difference before an undesired event actually has taken place. In real-world situations, manifested resilience can naturally be assessed post-facto, but such an assessment may not be very informative as there always will be a high degree uncertainty in relation to how similar future events will unfold.

Another challenging aspect is to determine what "good" performance is from a resilience point of view? To successfully cope with an unwanted situation is naturally a potential indicator but avoiding the situation altogether would be an even better outcome. Success must always be related to some form of criteria. Using the SyRes-model and the concept of core values as a point of departure, we can conclude that a system can be seen as resilient if it can uphold its core value(s) by implementing successful strategies before the situation spirals out of control. The ultimate goal of a system must always be survival, and hence even moving on the core value ladder can be seen as resilient behaviour as long as it is done in a graceful and controlled fashion.

This suggests that in order to assess resilient capability, even in a simulation, a thorough understanding of what a system must protect and preserve must be achieved when designing the simulation and the scenarios used in it. After this, sufficiently challenging events must be presented in the simulation so that the involved participants must cope with them by innovation and collaboration. Coping with challenges to core values by applying resilience strategies should hence be the main task for the participants.

In terms of assessment points, this tells us something about what can, and should, be assessed when applying scenario-based simulation approaches for training and researching resilience in the financial system. One crucial aspect will be to assess whether the participants were able to protect their core values. What strategies did the participants implement to handle the situation? Could they avoid undesired outcomes of the critical events designed into the scenario? If not, it should be assessed what happened if they failed – was the core value abandoned for another value further down the core value ladder? If so, how did this transition take place? In case of a complete breakdown of a core value, what were the consequences? Could the participant(s) recover and regain their earlier core values?

Further, it should be assessed if they managed to cope with specific events that were designed to challenge their ability to innovate and collaborate. If the event was designed in such a way that it demanded collaboration in order to be solved, how quickly was this collaboration established? Could the participants agree upon actions to be taken? Furthermore, if collaboration is required to uphold the core values and the collaboration with other actors failed, does this lead to cascade effects in other organizations and how can these be assessed?

On the behavioural level, assessments need to be made that evaluate if the participants develop and maintain sound team processes and a shared understanding of the current problems. There are several team cognition approaches that can be applied to assess these aspects (see for example Wildman et al, 2013). Of specific interest is shared understanding on the strategic level, as it provides an understanding of how well the team of participants share goals and objectives (Berggren, Johansson & Baroutsi, 2016). From a learning perspective, it is important that the learning goals are defined and assessed, and that the simulation environment allows for feedback and reflection. Both feedback and reflection are considered as fundamental for organizational learning (Gabelica et al., 2014; Knipfer et al., 2013). Feedback is also a central aspect to monitor and regulate work, as described in resilience theory (Hollnagel, Woods & Leveson, 2006; Lundberg & Johansson, 2015).

DISCUSSION

"Resilience Engineering" has existed as a term for at least ten years (Hollnagel, Woods & Leveson, 2006). The approach emerged as a reaction to the increasing complexity and intractability of socio-technical systems, as well as the inability of the contemporary theories and methods on safety to explain, and cope with, the same unpredictability. During the course of the last ten years, a multitude of theories and conceptual models explaining what resilience is have been developed (Bergström, van Winsen & Henriqsen, 2015; Soden et al., 2015). Unfortunately, less effort have been put in the "engineering" of resilience engineering, the development of methods and approaches aimed to strengthen the resilience of a system (Anderson, Ross & Jay, 2015; Wears & Bradley Morrison, 2015). This is perhaps not all that surprising, as some ambiguity still exist regarding exactly what is meant by resilience. Indeed, less focus needs to be put on collecting success stories and instead focus on "understanding how build adaptive capacity; how and when to trigger it; how to control it, and by what types of control architectures; and how to husband it for future use (as opposed to squandering it on the everyday)." (Wears & Bradley Morrison, 2015, p. 57). This paper has described an effort to develop experience-based training for improving resilience in collectives of organisations that jointly must cope with disturbances in critical infrastructures needed for upholding the fuel, food and payment systems.

However, as governance of infrastructures in the payment system is a poorly understood area, our objective is two-folded in the sense that the simulation and training environment can be seen as a "digital playground", where researchers and stakeholders can investigate various relationships between factors in the payment infrastructures. Encouraging stakeholder collaboration in a simulated gaming environment can thus be seen as a resilience-enhancing intervention, while at the same time providing an opportunity for researchers to collect unique data that can increase the understanding of resilience in highly networked environments. By adapting a simulation and gaming approach, the objective is to strengthen inter-organisational resilience by training decision makers through an experience-based training approach. This involves identification and development of methods for assessing resilience-related measures that can be used to assess training in the simulated environment.

Utilizing a simulated environment further allows for investigating the relationship between potential resilience and manifested resilience. It can naturally be argued that simulations never will be able to reflect the intricate complexity of real-world situations (Brehmer & Dörner, 1993). However, claiming that simulated environments are useless for investigating how resilience manifests itself in different situations is also flawed. Rather, it is the model underlying the simulated environment and the participation of relevant stakeholders that decide what conclusions that can be drawn from findings from such studies. In this case, our effort is to create an understanding of the core values of the stakeholders as well as the interdependencies between the different stakeholders and their ability to create resilience within their network(s). By understanding what the stakeholders in the payment system wants to protect and what trade-offs they are willing to engage in to preserve their core values, we will hopefully increase our understanding of what resilience means in these system(s).

Acknowledgements

The work reported in this paper is based on a grant from the Swedish Civil Contingency Agency.

REFERENCES

Anderson, J. E., Ross, A., & Jaye, P. (2015). Resilience engineering in healthcare: Moving from epistemology to theory and practice. *Proceedings of the 5th REA symposium*, Soesterberg, 25-27 June.

Ansell, C., Boin, A., & Keller, A. (2010). Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System. *Journal of Contingencies and Crisis Management*, 18: 195–207.

Basole, R. C., & Rouse, W. B. (2008). Complexity of service value networks: Conceptualization and empirical investigation. *IBM systems journal*, 47(1), 53-70.

Berggren, P., Johansson, B. J. E. & Baroutsi, N. (2016). Assessing the Quality of Shared Priorities in Teams Using

Content Analysis in a Microworld Experiment. *Theoretical Issues in Ergonomics Science* 18 (2): 128–46.

Bergström, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety*, 141, 131-141.

Brehmer, B., & Dörner, D. (1993). Experiments With Computer-Simulated Microworlds: Escaping Both the Narrow Straits of the Laboratory and the Deep Blue Sea of the Field Study. *Computers in Human Behaviour*, 9, 171-184.

Caluwé, L., Geurts, J., & Kleinlugtenbelt, W. (2012). Gaming Research in Policy and Organization. An Assessment From the Netherlands. *Simulation and Gaming*, 43(5), 600-626.

Cooke, N. J., & Shope, S. M. (2004). Designing Synthetic Task Environments. In S. G. Schiflett, L. R. Elliott, E. Salas, & M. D. Coovert (Eds.), *Scaled worlds: Development, validation, and application* (pp. 263–278).

Daalen, C. E., Schaffernicht, M., & Mayer, I. (2014). System Dynamics and Serious Games. *International Conference of the System Dynamics Society*, July 20-24, 2014

Gabelica, C., Van den Bossche, P., De Maeyer, S., Segers, M., & Gijselaers, W. (2014). The effect of team feedback and guided reflexivity on team performance change. *Learning and Instruction*, 34, 86–96.

Hollnagel, E. (2013). A tale of two safeties. *Nuclear Safety and Simulation*, 4(1), 1-9.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd.

Knipfer, K., Kump, B., Wessel, D., & Cress, U. (2013). Reflection as a catalyst for organisational learning. *Studies in Continuing Education*, 35(1), 30–48.

Kurapati, S., Lukosch, H., Verbraeck, A., & Brazier, F. M. T. (2015). Improving resilience in intermodal transport operations in seaports: a gaming approach. *EURO Journal on Decision Processes*, 3, 375–396.

Laere, J. van, Berggren, P., Gustavsson, P., Ibrahim, O., Johansson, B., Larsson, A., Lindqwister, T., Olson, L., & Wiberg, C. (2017). Challenges for critical infrastructure reslience: cascading effects of payment system disruptions. *Proceedings of ISCRAM 2017*, Albi, 21-24 May.

Laere, J. van, Vreede, G.J. de., & Sol, H.G. (2006). A social simulation game to explore future coordination in knowledge networks at the Amsterdam Police Force, *Journal of Production Planning and Control*, 17(6) 558-568

Lundberg, J., & Johansson, B. J. E. (2015). Systemic Resilience Model. *Reliability Engineering and Safety Science*. 141, 22-32.

Rome, E., Doll, T., Rilling, S., Sojeva, B., Voß, N., & Xie, J. (2016) The Use of What-If Analysis to Improve the Management of Crisis Situations. In Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): *Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach*, Springer.

Soden, R., Palen, L., Chase, C., Deniz, D., Arneson, E., Sprain, L., Goldstein, B.E., Liel, A., Javernick-Will, A., & Dashti, S. (2015). The Polyvocality of Resilience: Discovering a Research Agenda through Interdisciplinary Investigation & Community Engagement. *Proceedings of ISCRAM 2015*, Kristiansand, Norway, 24-27 May.

Wachs, P., Weber Righi, A., Abreu Saurin, T., Henriqson, E., Manzolli, A., Taborda, F., Tovar, R., Yukio Nara, F., Massashi Yamao, E., Tomal Ribas, L.G., & Fiejó Bório, H. (2016). Developing resilience skills through scenario-based training: A comparison between physical and virtual scenarios. *Proceedings of the 6th REA symposium*, Lisbon, 22-25 June.

Wears, R. L., & Bradley Morrison, J. (2015). Levels of resilience: Moving from resilience to resilience engineering. *Proceedings of the 5th REA symposium*. Soesterberg, 25-27 June.

Wildman, J. L., Salas, E., & Scott, C. P. R. (2014). Measuring Cognition in Teams A Cross-Domain Review. *Human Factors* 56 (5): 911–41.

IMPROVING TEAM RESILIENCE BY SUPPORTING MINDFUL COOPERATION AWARENESS

Christian Kunz, Toni Wäfler, Nina Saric and Katrin Fischer

Institute Humans in Complex Systems, School of Applied Psychology, University of Applied Sciences and Arts Northwestern Switzerland, Riggenbachstrasse 16, 4600 Olten, Switzerland

toni.waefler@fhnw.ch

www.fhnw.ch/miks

Abstract

Due to increasing complexity and changes of work in safety critical systems, organizational resilience is strongly influenced by the resilient cooperation in teams consisting of several experts. Through this cooperation, collective tacit knowledge evolves. A lack of systematic cultivation of such knowledge may cause disruptions in cooperation, finally reducing team resilience. Against this background in this project a method was developed and piloted that supports systematic cultivation of collective tacit knowledge. The method incorporates three parts: a pre-job workshop, a systematic exchange of cooperation relevant information during job execution, and a post-job workshop. The pilot showed that the method improves team resilience with regard to disruptions in cooperation. This can be achieved by systematic elicitation, sharing and joint handling of collective tacit knowledge. In this process, mindfulness with regard to (in-)compatibility of mutual expectations between team members and awareness regarding successful cooperation (cooperation awareness) are systematically fostered. Furthermore, organizations get the opportunity to learn from tacit knowledge based local adaptations as well as to identify conflicts between being resilient and ensuring compliance to standards at the sharp end. This enables taking the right measures to foster team resilience by supporting mindful cooperation awareness.

INTRODUCTION

Increasing complexity of technical facilities and organizational processes changes work in safety critical systems. In respective organizations, many tasks have become too complex to be successfully performed by only one person. This brings about both, an increasing specialization regarding expertise as well as increasing division of labor. Consequently, many tasks have to be performed by teams consisting of several experts with specific expertise. This makes cooperation of different experts more needed, but also more demanding.

Hence, cooperation of experts has become a crucial success factor for the achievement of common objectives in complex, safety critical systems. For this reason, the resilience of an organization is strongly influenced by the resilient cooperation in teams consisting of several experts. At the same time, many organizations - maybe trapped in Safety-I thinking (Hollnagel, 2012) - aim at assuring safety by implementing more prescriptive standards and by expecting experts to comply with those. Thereby, the teams' ability to adapt to dynamic work conditions may be impeded, and, thus, the teams cannot cope resiliently with challenges and opportunities of the work context. Resilience potential of teams and organisations can hardly be enacted that way.

The Role of a Team's Collective Tacit Knowledge Regarding Resilient Cooperation

Resilient teams are able to adapt to dynamic work conditions (Rankin, Lundberg & Woltjer, 2014). This ability emerges from team members' cooperation. Through cooperation teams also develop collective (embedded, see Lam, 2000) tacit knowledge.

Collective tacit knowledge is the situated and coordinated interaction of different experts' individual tacit knowledge with regard to the achievement of common objectives in a certain work process. It evolves from the repeated cooperation of the same experts in a particular team. It incorporates individual tacit knowledge regarding jointly developed local adaptation strategies which have (unconsciously) creeped in over time, and which are aligned with actual work requirements at the sharp end. This kind of knowledge qualifies a team and its members for synergetic acting based on respective adaptation strategies. It enables successful cooperation without the requirement for explicit coordination. This makes a team more resilient, i.e., more adapted to actual work requirements and more effective with regard to the achievement of common objectives.

Key aspects of collective tacit knowledge are (a) team specific cooperation patterns, (b) individual experiences from previous cooperation and mutual expectations regarding future cooperation in the team, (c) mindful cooperation awareness and compatibility of individual expectations and, thus, (d) synergetic acting in cooperation. In the following, the key aspects and their interrelations are outlined. Furthermore, it is described, why a systematic cultivation of collective tacit knowledge is crucial for fostering resilient cooperation in teams.

a) Team Specific Cooperation Patterns

When the same people repeatedly work together over a longer time period, team specific patterns of cooperation evolve. Team specific cooperation patterns are coordinated behaviour patterns (routines, see Grote, 2009) - e.g. for cooperatively mastering certain tasks or problems - which over time consciously or unconsciously creeped in cooperation. These patterns reflect cooperative adaptations to dynamic work conditions thereby fostering team resilience (see Rankin et al., 2014). Over time these adaptation strategies are individually - and mainly unconsciously - considered normal and taken for granted (Grote, 2009). Sometimes these adaptations do not entirely comply with prescriptive standards. An example is, when two experts first work together according to prescriptive standards and fail to achieve objectives in the required time and - over time - learn (consciously or unconsciously) that cooperation is more resilient (i.e. adapted to time pressure) when they deviate from the standard. As a consequence, this deviation may become normalized and hence create the basis for a tacit pattern of cooperation among the involved experts.

b) Individual Experiences from Previous Cooperation and Mutual Expectations Regarding Future Cooperation in the Team

On the basis of the team specific cooperation patterns, team members - over time and with repeated cooperation - develop specific experiences regarding the cooperation in the team. On that basis, they individually and often unconsciously develop specific expectations regarding future cooperation within the team as they expect that cooperation in future will work very similarly as in the past. Such, team specific cooperation patterns, which creeped in over time, trigger mutual expectations among team members (see Spiess, 1998; Tjosvold, 1988; Weick & Sutcliffe, 2007). According to Weick and Sutcliffe (2007) expectations are built into organization roles, routines, and strategies. They create the orderliness and predictability that people count on when they work together. They serve as implicit assumptions that guide behavioural choices. Therefore, individual cooperation behaviour is guided by the individual (and mainly unconscious) expectations every team member has developed regarding successful cooperation with the other team members.

c) Mindful Cooperation Awareness and Compatibility of Individual Expectations

Team specific cooperation patterns, individual experiences regarding these cooperation patterns and the triggered mutual expectations regarding future cooperation in the team are key elements of successful cooperation. However, individual experiences regarding these team specific cooperation patterns and, thus, the team members' mutual expectations regarding cooperation can be more or less compatible. Incompatibilities can lead to disruptions in cooperation because mutual expectations and the following cooperation behaviour do not sufficiently interact. However, the compatibility of mutual expectations is according to the Distributed Situation Awareness Theory (Salmon, Stanton, Walker & Jenkins, 2009) paramount for successful cooperation and, consequently, for the resilience of teams.

Mindful cooperation awareness is the continuously and mindfully updated and reconciled awareness of team members regarding successful cooperation, especially regarding (in-)compatibility of (tacit) mutual expectations in cooperation (Salmon et al., 2009; Weick & Sutcliffe, 2001, 2006, 2007). "Reconciled" means, according to Salmon et al. (2009), that cooperation relevant information is systematically exchanged and concerted between cooperation partners.

Incompatibilities of mutual expectations can be recognized when team members are mindful regarding such incompatibilities. Mindfulness is according to Krieger (2005, p. 127, quoted by Weick & Sutcliffe, 2006) "a psychological state in which individuals engage in active information processing while performing their current tasks such that they are actively analyzing, categorizing, and making distinctions in data (p. 516)". According to Weick and Sutcliffe (2001, p. 42) mindfulness furthermore is "the combination of ongoing scrutiny of existing expectations, continuous refinement and differentiation of expectations based on newer experiences, willing-ness and capability to invent new expectations that make sense of unprecedented events, a more nuanced appreciation of context and ways to deal with it, and identification of new dimensions of context that improve foresight and current functioning". Mindful teams are regularly and robustly discussing potential threats to reliability, develop a nuanced and current understanding of the context by frequently questioning the adequacy of existing assumptions (expectations) and integrate these understandings into an up-to-date big picture (Vogus & Sutcliffe, 2012). Regarding collective tacit knowledge, mindful teams uncover early signs that expectations are inadequate. Therefore, individual uncertainties regarding cooperation are early signs (leemers, see Weick & Sutcliffe, 2007) that mutual expectations regarding cooperation may not be compatible. Such, uncertainties are an indicator for potential threats to successful cooperation in the team (Vogus & Sutcliffe, 2012; Weick & Sutcliffe, 2007).

According to these concepts, mindfulness in cooperation is an active processing of cooperation relevant information especially regarding (in-)compatibility of (tacit) mutual expectations among team members. In this process, awareness regarding successful cooperation is created in a mindful way, or, i.e., mindful cooperation awareness is built (Salmon et al., 2009; Vogus & Sutcliffe, 2012; Weick & Sutcliffe, 2001, 2006, 2007).

d) Synergetic Acting

Synergetic acting is the result of successful cooperation in a team when aiming to achieve common objectives. It emerges from collective tacit knowledge on the basis of team specific cooperation patterns (routines, see Grote, 2009), mindfully reconciled cooperation awareness, and, thus, compatible mutual expectations regarding cooperation in the team (Salmon et al., 2009; Spiess, 1998; Tjosvold, 1988). It enables a team to successfully cooperate without the requirement for explicit coordination. This makes a team efficient and effective regarding achievement of common objectives and fosters team resilience.

A lack of systematic cultivation of collective tacit knowledge in a team may cause disruptions in cooperation, e.g. in case of staff fluctuation. New team members unfamiliar with the team specific cooperation patterns may base their actions on prescriptive standards while, at the same time, long-time team members behave according to the patterns that creeped in over time. This can lead to an incompatibility in mutual expectations causing disruptions in cooperation (e.g. misunderstandings, unintentional negligence or omissions). Such, disruptions can reflect conflicts between being resilient and complying with standards. This is the case, when team specific cooperation patterns - which reflect cooperative adaptations to dynamic work conditions thereby fostering team resilience (Rankin et al., 2014) - are not reconciled with prescriptive standards and, thus, do not entirely comply with those. As a result, the gap between work as done and work as imagined increases (Dekker, 2006). Incompatibilities which are not recognized and the potentially resulting disruptions can finally reduce team resilience. Therefore, a systematic cultivation of collective tacit knowledge is crucial for fostering resilient cooperation in teams (team resilience) and, thus, an organization's resilience. In this process, mindful cooperation awareness is built.

DEVELOPED AND PILOT TESTED METHOD

On the basis of the descriptions above a method was developed and piloted in this project that supports systematic cultivation of collective tacit knowledge. It is presented in the following sections.

The Method's Basic Concept And Goals

The method developed in this project supports the elicitation (Nonaka & Takeuchi, 1995), the sharing and the joint handling of collective tacit knowledge as well as of potential uncertainties (leemers, see Weick & Sutcliffe, 2007). Elicitation means according to the SECI-Model of Nonaka & Takeuchi (1995) to grasp and to document experience-based knowledge of experts - that is tacit and therefore difficult to articulate - in a systematic way that enables further use. Beside this, the aim of the systematic cultivation of collective tacit knowledge is (a) to systematically enhance the team members' mindful cooperation awareness regarding successful cooperation, (b) to reveal and to deal with incompatible expectations, and (c) to prevent potential disruptions in cooperation in a proactive manner.

The method incorporates three parts: a pre-job workshop, a systematic exchange of tacit knowledge and mutual expectations during job execution and a post-job workshop. The three parts build on one another supporting a stepwise deepening of a mindful cooperation awareness.

Pre-job workshop

The pre-job workshop is a workshop with all members of a team the particular work process of which is subject of the method's application. The aims are (a) the first-time elicitation of individual as well as collective tacit knowledge, (b) the documentation of the elicited knowledge using specific template cards, and (c) the team members' sensitization regarding aspects relevant for successful cooperation.

The workshop's methodology is based on group discussions (Flick, 2009) as well as on the principles of storytelling (Nielsen & Madsen, 2006), group storytelling (Santoro & Brézillon, 2005), causal mapping (Ambrosini & Bowman, 2001), and the self-q-technique (Katenkamp, 2011). According to these methods, tacit knowledge can be elicited by generating story-like narratives as well as by a stepwise question-based deepening approach.

In the first workshop-part individual tacit knowledge is elicited by discussing a fictitious but realistic scenario facilitated by reflection-promoting questions. The fictitious scenario contains a short-term absence of an experienced team member who is replaced by an unexperienced colleague. Every team member thereby takes - fictitiously - the role of the experienced and the absent person. Based on this scenario it is individually reflected and subsequently discussed where the unexperienced colleague could disrupt cooperation if he bases his actions on prescriptive standards only (e.g. work instructions or checklists), which experiences the unexperienced colleague would initially be lacking for successfully cooperating with the other experienced team members, and which important and success relevant advice, that can't be find in any official document, the unexperienced colleague needs for successfully cooperating in the team. The stepwise elicited knowledge is individually documented on specific template cards.

In the second part of the workshop the team's collective tacit knowledge is elicited. In detail, mutual expectations as well as uncertainties regarding the cooperation (leemers, see Weick & Sutcliffe, 2007) are elicited by using question-based group discussions. The questions guide the team members to imagine the upcoming cooperation in the team and to think about; (1) which team specific cooperation patterns exist in the cooperation, (2) thus, which concrete mutual expectations regarding upcoming cooperation in the team exist, (3) what new team members, that are not yet familiar with these cooperation patterns, can't know regarding these patterns, (4) which kind of disruptions in cooperation could occur because of incompatible experiences and expectations between team members, and finally (5) which uncertainties regarding the upcoming cooperation team members have at the moment. Discussing these questions enables an elicitation of collective tacit knowledge, i.e. of concrete expectations regarding the cooperation in the team. Furthermore, uncertainties regarding upcoming cooperation are revealed. The elicited expectations as well as uncertainties are finally documented in the form of messages between team members using specific template cards.

Systematic Exchange of Cooperation Relevant Information During Job Execution

The systematic exchange of cooperation relevant information during job execution builds on the elaborated content from the pre-job workshop. It contains an exchange and answering of the individually developed messages. Therefore, three short interviews (10 - 15 minutes) with each team member are conducted. The interviews are optimally timed shortly before cooperation starts, during cooperation, and shortly after cooperation has finished. The aims are (a) to recognize and to deal with incompatible expectations among team members in a mindful and resilient way, (b) to resolve uncertainties regarding upcoming cooperation, (c) to develop and to document individual learnings regarding past cooperation in the team, and thereby (d) to support team members' mindful cooperation awareness.

The short interviews are based on interview guidelines containing three parts. The first part is a look back to the cooperation experienced in the team up to the moment of the interview. It contains questions regarding the reasons for successful or not successful cooperation in the past and the learnings that can be taken for future cooperation. The learnings are documented in a personal learning form. The second part focuses on the messages elaborated in the pre-job workshop. Together with the interviewee, the messages he received from the other team members containing concrete expectations as well as uncertainties are processed and answered. The third part contains a quick outlook to the upcoming cooperation. Thereby, remaining or newly recognized uncertainties regarding the cooperation in the team are elicited and, again, documented in the form of messages to the respective team member(s).

Post-Job Workshop

The post-job workshop builds on the elaborated content from the pre-job workshop and the short interviews. It is - like the pre-job workshop - a workshop with all members of a team the work process of which is subject of the method's application. The aims are (a) to derive collective learnings from the elicited knowledge as well as from the cooperation experienced in the working process and (b) to define concrete measures to promote the interpersonal knowledge exchange as well as to improve the cooperation within the team.

In the first part of the workshop, collective as well as individual learnings based on the elaborated content are derived and documented using a facilitated group discussion based on specific questions. For doing this, the messages and related answers (see method of the systemic exchange above) are studied by all team members and emerging questions are answered. Then, the team members are instructed, first individually and then together in the group, to identify conclusions for future cooperation in the team. The group discussion is guided by the questions regarding: (1) what needs to be considered particularly in future cooperation (2) what are areas for improvement regarding successful cooperation, and finally (3) what was successful and therefore needs to be sustained in future cooperation. The collective learnings are documented using specific template cards.

On this basis, in the second part of the workshop, collective and concrete measures to promote the interpersonal knowledge exchange as well as to improve the cooperation within the team are defined. The concrete measures include clear responsibilities as well as deadlines for implementation.

Result of Pilot Test

The pilot showed that the method supports systematic cultivation of collective tacit knowledge. It supports the elicitation, the sharing and the joint handling of collective tacit knowledge as well as of potential uncertainties regarding cooperation. By doing this, team specific cooperation patterns that consciously or unconsciously creeped in over time, mutual expectations regarding future cooperation that team members often unconsciously developed (on the basis of the cooperation they experienced in the team) as well as uncertainties regarding upcoming cooperation are elicited and jointly handled.

Furthermore, the pilot showed that implementing a systematic exchange of the elicited cooperation relevant information enables an ongoing monitoring of mutual expectations and uncertainties regarding cooperation. Thereby, individuals engage in active information processing (Weick & Sutcliffe, 2006) enabling a continuous update and reconciliation of cooperation relevant information between team members. Ongoing scrutiny of existing expectations and continuous refinement and differentiation of expectations based on newer experiences (see Weick & Sutcliffe, 2001) are stressed. Such, incompatibility in mutual expectations can be revealed and proactive measures can be taken to avoid disruptions in cooperation. In this process, mindfulness regarding (in-)compatibility of expectations among team members and awareness regarding successful cooperation are systematically supported (see Salmon et al., 2009; Vogus & Sutcliffe, 2012; Weick & Sutcliffe, 2001, 2006, 2007).

CONCLUSION

A regular application of the developed and pilot tested method and in doing so a systematic cultivation of collective tacit knowledge provides the following advantages.

On the individual level, employees continuously learn from cooperation in the team. They are - individually and in exchange with their cooperation partners - on a regular basis systematically guided to question the adequacy of personal experiences from previous cooperation with regard to local adaptation strategies as well as of mutual expectations regarding future cooperation. They become increasingly sensitized to success-relevant aspects in cooperation which normally are not taken into account. Thereby, they develop more and more mindfulness regarding these aspects, especially regarding (in-)compatibility of (tacit) expectations among team members. As a result, they develop mindful cooperation awareness and capabilities to uncover early signs for potential threats to successful cooperation in the team (Vogus & Sutcliffe, 2012; Weick & Sutcliffe, 2007).

On the level of teams, team specific cooperation patterns that unconsciously creeped in over time and that may not entirely comply with prescriptive standards can be jointly revealed. Thereby, conflicts between local adaptation and compliance with prescriptive standards are identified. Furthermore, implementing a continuous and systematic exchange of cooperation relevant information fosters a mindful update and reconciliation of cooperation awareness (Salmon et al., 2009; Vogus & Sutcliffe, 2012; Weick & Sutcliffe, 2001, 2006, 2007). This has the potential for improving team resilience: actual cooperation can be continuously monitored on the basis of elicited, cooperation relevant information (i.e. individual experiences, expectations as well as uncertainties). Thereby, incompatibility in mutual expectations can be recognized and potential disruptions can be anticipated early. This enables taking of proactive measures to avoid disruptions in cooperation (e.g. in case of staff fluctuation), i.e. responding to anticipated disruptions to promote safe and successful cooperation. Teams and its members are empowered to recognize conflicts between being resilient and ensuring compliance at an early stage.

On the organizational level, the opportunity to learn from tacit knowledge based local adaptations is created. This in turn can be taken as an opportunity for questioning the adequacy of prescriptive standards in view of actual requirements at the sharp end. Conflicts on various levels between being resilient and ensuring compliance can be recognized. Furthermore, organizations can learn from what goes right thereby adopting more and more Safety-II thinking (Dekker, Hollnagel, Woods & Cook, 2008; Hollnagel, 2012). On that basis measures can be taken for balancing the pressure of being resilient and, at the same time, ensuring compliance. Such, resilient adapting and complying with prescriptive standards are not necessarily contradictive. Teams can be explicitely supported in their ability to resiliently adapt to dynamic work conditions (Rankin et al., 2014), when adaptation strategies are elicited and systematically reconciled with prescriptive standards. By doing so, the team can cope resiliently with challenges and opportunities in the work context and conflicts between being resilient and ensuring compliance can be resolved. Hence, the gap between work as imagined and work as done (Dekker, 2006) can be reduced and the resilience potential of teams can be enacted by supporting mindful cooperation awareness.

REFERENCES

Ambrosini, V. & Bowman, C. (2001). Tacit Knowledge: Some Suggestions for Operationalization. *Journal of Management Studies, 38*, 811-829.

Dekker, S. A. (2006). Resilience Engineering: Chronicling the Emergence of Confused Consensus. In E. Hollnagel, D. D. Woods & N. Leveson (Ed.), *Resilience Engineering - Concepts and Precepts* (pp. 77-92). Farnham, UK: Ashgate.

Dekker, S. A., Hollnagel, E., Woods, D. D. & Cook, R. (2008). *Resilience Engineering: New directions for measuring and maintaining safety in complex systems* (Final Report, November 2008). Lund, Sweden: Lund University, School of Aviation.

Flick, U. (2009). *Qualitative Sozialforschung: Eine Einführung (2. Auflage)*. Hamburg: Rowohlts.

Grote, G. (2009). *Management of Uncertainty: Theory and Application in the Design of Systems and Organizations*. London: Springer.

Hollnagel, E. (2012a). *A Tale of Two Safeties. The Resilient Health Care Net*. http://www.resilienthealthcare.net/A_tale_of_two_safeties.pdf, accessed on 10-04-15.

Katenkamp, O. (2011). *Implizites Wissen in Organisationen*. Wiesbaden: VS Verlag.

Lam, A. (2000). *Tacit Knowledge, Organizational Learning and Societal Institutions: An Integrated Framework*. http://oss.sagepub.com/content/21/3/487, accessed on 04-02-17.

Nielsen, L. & Madsen, S. (2006). *Storytelling as Method for Sharing Knowledge across IT Projects*. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1579677&tag=1, accessed on 15-03-17.

Nonaka, I., Takeuchi, H. (1995). *The Knowledge-creating Company: How Japanese Companies Create the Dynamics of Innovation.* Oxford: Oxford University Press.

Rankin, A., Lundberg, J. & Woltjer, R. (2014). A Framework for Learning from Adaptive Performance. In C. P. Nemeth & E. Hollnagel (Ed.), *Resilience Engineering in Practice, Volume 2, Becoming Resilient* (pp. 79-96). Farnham, UK: Ashgate.

Salmon, P. M., Stanton, N. A., Walker, G. H. & Jenkins, D. P. (2009). *Distributed Situation Awareness: Theory, Measurement and Application to Teamwork*. Farnham: Ashgate.

Santoro, F. & Brézillon, P. (2005). *Group Storytelling Approach to Collect Contextualized Shared Knowledge*. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1508303, accessed on 16-03-17.

Spiess, E. (1998). *Formen der Kooperation - Bedingungen und Perspektiven*. Göttingen: Hogrefe.

Tjosvold, D. (1984). Cooperation theory and organizations. *Human Relations, 37*, 743-767.

Vogus, T. J. & Sutcliffe, K. M. (2012). Organizational Mindfulness and Mindful Organizing: A Reconciliation and Path Forward. *Academy of Management Learning & Education, Vol. 11*, No. 4, 722-735.

Weick, K. E. & Sutcliffe, K. M. (2001). *Managing the Unexpected.* San Francisco: Jossey-Bass.

Weick, K. E. & Sutcliffe, K. M. (2006). Mindfulness and the Quality of Organizational Attention. *Organizational Science, Vol. 17*, No. 4, 514-524.

Weick, K. E. & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. San Francisco: Jossey-Bass.

ORGANIZATIONAL RESILIENCE

Christopher Nemeth, PhD[1], Beth Lay[2], Jennifer Blume, PhD[3], Jerri Stephenson[4], Jon Holbrook, PhD[5]

1 Applied Research Associates, Inc., 2760 Eisenhower Highway, Alexandria, VA, USA

1 cnemeth@ara.com

2 Applied Resilience, 404 Emerson Street, Houston, TX USA

2 Elizabeth.A.Lay@hotmail.com

3 Raytheon Corporation, Huntsville, AL, USA

3 Jennifer.L.Blume@raytheon.com

4 NASA Johnson Space Center, Houston, TX, USA

4 jerri.l.stephenson@nasa.gov

5 NASA Langley Research Center, Hampton, VA, USA

5 jon.holbrook@nasa.gov

Abstract

Understanding high risk work settings from the viewpoint of resilience engineering (RE) requires methods that enable the researcher to successfully collect and analyze data, then provide well-founded findings and recommendations. We report on our experience using one RE method, the Resilience Analysis Grid (RAG) to assess the organizational resilience of the role the U.S. National Aeronautics and Space Administration (NASA) plays as a partner in the International Space Station (ISS) Program. In 2013, a potentially dangerous amount of water was observed to accumulate in an astronaut's helmet during a spacewalk. After an investigation of this mishap, the assessment team leader selected the RAG to analyse NASA performance in routine ISS operations. The team used the four RAG cornerstones (anticipate, monitor, respond, learn) to structure data collection, analyses, and findings. We reflect on the application of the RAG to study a complex, high risk work setting and share our experience with introducing team members to RE in general, as well as the RAG in particular.

1. INTRODUCTION

The National Aeronautics and Space Administration (NASA) has supported the US mission to achieve human space flight since 1958 through the Mercury, Gemini, Apollo, Space Shuttle and International Space Station (ISS) programs. NASA's many accomplishments, including lunar landings, have demonstrated remarkable success in accomplishing high risk ventures. NASA's history, however, has also demonstrated how failure to learn from past events and manage risks can threaten future missions.

1.1 Shuttle Mishaps

On January 28, 1986, the space shuttle Challenger broke apart 73 seconds after the liftoff of Shuttle orbiter mission STS-51-L. The Rogers Commission report (Rogers Report, 1986) cited multiple contributors: flawed decision making (from communication failures, incomplete and misleading information, poor management judgement), missed warning signs (accepting unsafe flight risks), a silent safety culture, production pressures (compressed training schedules, focus on short term resource shortages) and overconfidence in past success. NASA responded by creating the Office of Safety & Mission Assurance.

On February 1, 2003, the space shuttle Columbia disintegrated upon reentering the Earth's atmosphere. The Investigation Board report (CAIB, 2003) cited multiple causes including normalization of deviance, shuttle program complacency, and a broken safety culture. NASA responded by creating the NASA Engineering and Safety Center (NESC) as an independently funded program composed of technical experts to fill the need for an independent resource to provide an alternative perspectives on complex technical issues.

1.2 The International Space Station

The ISS is a habitable artificial satellite within a multifaceted, international sociotechnical system that is partly run by the NASA ISS Program. Crew members have inhabited and continuously operated the ISS in low space orbit altitude (249 mi) since late 2000. Members of the ground control staff are based in Johnson Space Center, in Houston, TX.

Figure 1 : *The International Space Station (NASA 2017)*

Figure 2. *Water in helmet* of *EVA23 astronaut (MIB 2013)*

1.3 Extravehicular Activity (EVA) 23

On July 16, 2013, two US crew members performed maintenance tasks outside of the ISS during Extravehicular Activity (EVA) 23. Forty-four minutes into the EVA, a crew member reported water from an unidentified source inside of his helmet at the back of his head. The crew member continued working, but the amount of water increased and moved to his face, creating a potential suffocation hazard. The EVA was terminated and the crew members returned to the ISS.

The post-EVA debrief revealed that the water covering his eyes, nose and ears had impaired the crew member's visibility and breathing. A Mishap Investigation Board (MIB) later identified what caused the situation and made 19 recommendations that NASA could implement to prevent future similar mishaps. ISS program management approached the NESC after the MIB to provide an objective engineering and safety assessment of the ISS organization in the wake of the EVA 23 incident. The assessment project lead saw the use of resilience engineering as an opportunity to obtain insights into the issue beyond what conventional risk management approaches would normally offer.

1.4. Scope and value

Even though resilience engineering research has identified resilient performance for years in a number of high-risk sectors (Nemeth & Herrera, 2015), few methods such as the Functional Resonance Analysis Method (Hollnagel 2012) and the Resilience Analysis Grid (RAG) (Hollnagel 2011) are specific to resilience engineering (RE). The RAG's simplicity and relatively recent introduction provided the team with the opportunity to use it to study an aerospace application and to try it with team members who were unfamiliar with RE. Results from team member experience using the RAG would provide insights into the method's strengths and any potential opportunities to enrich it.

2. RESEARCH DESIGN AND METHODS

2.1 Preparation

NASA has developed extensive flight rules and procedures through the decades to manage high risk operations, yet the accumulation of water during EVA 23, as well as during EVA 22 shortly before, fell outside of ISS procedures. The Mishap Investigation Board (MIB) Chair asked during a briefing on EVA 23 (Hansen, 2013) "…why do we keep having these tragedies and not learning the lessons they are teaching us?" In addition, an experienced assessment team member mentioned that the EVA 23 report was like many other mishap reports, suggesting that NASA does not always change what it does even after evidence from near-misses that threats to mission performance have occurred. The team member drew the comparison to "plan continuation errors", which are decisions to continue with a plan despite cues in the environment that suggest changing the course of action (e.g., Orasanu, Martin, & Davison, 2001).

This assessment study sought to look beyond simple adaptation to learn "…how well can a system handle disruptions and variations that fall outside of the base mechanisms/model for being adaptive as defined in that system" (Woods, 2012). Our understanding of the issues that the ISS organization confronted during EVA 22 and 23 led us to identify two research questions to guide our study:

- How does ISS handle weak signals that indicate potential safety threats?
- How does ISS balance ongoing resource constraints with production pressures?

We used the four RAG cornerstones to detail how we would seek the data. Table 1 shows an example of how the cornerstone «anticipate» was used to structure inquiry.

Table 1: Use of RAG Cornerstone

	Issue Number/Issue	Research Query	Source
Anticipate	M2a Who is watching what? Is there a monitoring plan?	What constitutes a signal that a potential threat to safety exists?	Interview
	M2b How does ISS allocate attention? Reallocate attention?	What is a "weak" safety signal?	Interview
		Who is responsible for safety signals?	Artifact, Interview

Interview Guide

Development and use of a guide ensured that interviews would collect data consistently across participants and provide answers to the research questions. Rather than limiting inquiry, the guide's structure ensured a consistent approach among the interviews so that the team could identify and tabulate patterns during the analysis phase. One team member conducted a pilot interview with a NASA contractor to demonstrate how to perform an interview using the guide.

2.2 Data Collection

The assessment team collected data in 3 ways: 1) structured interviews with ISS staff members, 2) direct observation of real-time ISS operations, and 3) analysis of ISS documents, presentations, and meeting transcripts.

Structured Interviews

Assessment team members conducted structured interviews with 17 NASA staff members who directly supported ISS in one of 8 roles: Flight Crew, Flight Director, Increment Manager, Mission Evaluation Room (MER) Manager, Operations Planner, Safety, Engineering, and Training. To identify interview candidates, the team lead sent email requests to ISS Branch leads at JSC in Houston. The request included the study's purpose, the expected length of the interview (90 minutes), and a request for contact information for up to 3 Branch members who might be available to participate. All interviews took place during 1 of 3 week-long assessment team visits to JSC. Once the team lead received contact information, he arranged a 90-minute block of time with each participant during one of the team's site visits.

Team members conducted individual interviews with all participants. One team member performed as lead interviewer, accompanied by one or more note takers who used word processing software on laptop computers to record interview questions and responses in real time. Notes included a mix of verbatim and paraphrased participant responses. Across the 17 interviews, all assessment team members served in both roles. Before each interview began, the lead interviewer briefed the participant on the study's purpose and introduced other assessment team members who were present. Participants were assured that they would not be identified personally in our analysis, and they were free to withdraw or end the interview at any time.

Observations

Over the course of the project, assessment team members observed four Extra-Vehicular Activities (EVAs) and one visiting-vehicle event (cargo vehicle berth) from two locations within the Mission Control Center at JSC: the observation room overlooking the Mission Control "floor," and a conference room inside the MER, station-to-ground voice loops were also available in both locations. Assessment team members also attended an EVA readiness review, and a post-EVA debrief in the MER. These observations helped the assessment team to better understand the flow and pace of real-time ISS operations. Notes team members took during these observations were available to supplement, support, and interpret interview data.

Artifact Analysis

The team also considered archival data ISS staff members had produced. These included the EVA 23 Mishap Investigation Board report (NASA, 2013), the Corrective Action Plan detailing ISS Program responses to the EVA 23 MIB Recommendations, and an audio recording of the ISS Mission Management Team (IMMT) EVA 23 go/no-go meeting. As with real-time observations, analysis of these archival data was available to supplement, support, and interpret data from the structured interviews.

2.3 Data Analysis

Analysis of data from the team's collection efforts translated observed phenomena into findings that describe the ISS organization. The team used thematic analysis, which is "… a method for identifying, analysing, and reporting patterns (themes) within data. It minimally organises and describes your data set in (rich) detail" (Braun & Clarke 2006). The following analysis phases ensured that the process was rigorous and maintained continuity from data, through analysis, to themes, findings, and recommendations.

Systematic data review and coding

We copied content from each team member who took notes during an interview into a common file for each interviewee, identifying which of the two research questions and which of the four cornerstones the data point addresses. We sorted notes from each team member according to interview topics, organized along the same lines as the interview guide. We then identified, from among all of the team member notes for a particular topic, what went well, as well as instances that affected ISS ability to adapt. Using the thematic categories developed during the team working session, we coded interview sections according to their relevance to one or more themes.

Review and interpretation of coded data

With a consensus set of themes, each research team member was assigned a subset of the data excerpts to review and interpret. Analyses coded data according to the research question(s) it addressed, and which RAG cornerstones it related to. We then collected the key data points into a common file of all subjects who have the same role (e.g., flight director).

Synthesis and integration

With all data assembled according to roles, team members were then assigned separate sets to review and write insights: summary statements that drew from the data to address the research questions. Some of the data points could apply to more than one insight. In the final phase of analysis, insights from all team members were clustered into 52 sets with similar meanings, and their similarity was confirmed by being able to represent them with an "integrated insights" statement.

Findings

Two team members then reviewed all insights, merged them into 26 groups according to the research questions and RAG, and wrote findings statements. Statements noted resilient performance, needs for improvement, and implications that pointed toward recommendations. These conclusions into the actual nature of NASA and ISS performance were based on the above analyses, which included data drawn from artifacts and interviews. Recommendations were couched in terms of RE, and nature and implications of NASA/ISS ability to adapt and how that affects ISS ability to anticipate, monitor, respond to, and learn from unanticipated challenges.

3. DISCUSSION

Except for two consultants, members of the assessment team were initially unfamiliar with resilience engineering. This provided us with the opportunity to introduce team members to RE as a concept, and the RAG as an RE method.

3.1 RAG Strengths

Our experience using the RAG revealed a number of aspects that served the team well through the study.

Simplicity

The RAG concept can be expressed in one chapter, using four essential aspects to understand a complex high-hazard system. Team members were able to start to use the RAG soon after learning about it.

Accessibility

The use of plain language terms for each cornerstone made it possible for less experienced team members to understand how to use them.

Veracity
The four cornerstones enabled team members to accurately call out aspects of, and impediments to, resilient performance without the need to create additional terms or workarounds.

Support for qualitative and quantitative inquiry

The RAG can support both quantitative as well as qualitative system analyses. Hollnagel (2015) describes how Likert-style ratings can be used to develop value estimates of the required abilities. The values can be used to construct representations, such as polar diagrams or "radar charts." The assessment team for this project relied on verbal descriptions to elicit ISS organization nuances and complexities, then produced the data-insights-findings-recommendations structure it has been asked to provide.

3.2 RAG Opportunities

There were a few aspects of the RAG that the study team found challenging, and might provide an opportunity for further development.

Tacit Knowledge
While team member backgrounds included cognitive science, psychology, or human factors, some members found it necessary to know more about RE than what the cornerstones alone represented. Team members who had more experience with RE were able to provide context on RE. Members reviewed several articles that described fundamental concepts of RE, and the RE consultants shared examples and described resilience and brittleness as opportunities arose. Future publication on RE might provide deeper explanations so that those who are new to the RAG might absorb it more readily.

Examples
Team members who were new to RE found it a challenge to get the "big picture" of how to use the RAG. Examples of performance or behavior or practices that are specific to the domain being studied could be used to describe each RAG cornerstone in terms of whether or not it facilitates resilience. Providing this kind of structure early in a project could enable team members who are not familiar with RE to be better informed when planning data collection and analysis. Applications such as this study and future studies can provide examples for others who may be unfamiliar with the RAG to use the method.

Software support
The team successfully used Microsoft Excel to manually manage data analysis. Commercially available qualitative analysis software programs that are designed to support thematic analysis (e.g. Dedoose, www.dedoose.com) can facilitate the coding, tracking, and management process from data to themes, insights, findings, and recommendations.

3.3 Team Use of RAG
Prior studies such as Aaen-Stockdale (2014) and Ljunberg & Lundh (2013) have used the RAG to understand clearly bounded systems or processes with questions that were designed for use in a survey with quantitative data results depicted in polar diagrams. For example, questions related to "monitor" ask how indicators have been defined, how often revised, how many in the design of are leading or lagging, etc. By contrast, our team used a more open-ended approach, using the RAG cornerstones to organize the interview guide to answer the 2 research questions (RQ). Table 2 compares the two approaches using the RAG.

Table 2: Prior RAG Studies and NASA Study Comparison

Prior RAG Studies	*ISS study*
RAG process structured with detailed questions, possibly applied in survey format.	RAG process shaped a flexible interview process. Analysis was deliberately unstructured to benefit from the diversity of team member backgrounds and avoid biasing outcomes.
Boundaries well defined, process focused	Boundary / scope of project was broad and loosely defined
Investigative, quantitative	Explorative, qualitative

Table 3 shows how the ISS study interview guide spelled out questions (“Interviewer asks”) the interviewer would use to elicit a response form the participant, and how responses could be used to inform the research question (“Interviewer listens for”), and which RQ and RAG cornerstone were pertinent.

Table 3: Interview Guide Structure

General Topic	*Interviewer asks*	*Interviewer listens for*	*Relevant to RQ 1*	*Relevant to RQ 2*	*RAG*
Roles and Responsibilities	Please briefly describe your role on the ISS team and how it relates to mission safety.	How do new/diverse team members participate in ISS operations?	X		M

Unique Contribution of RE

We found several similarities in observations when we compared our study’s findings to the lesson learned presentation for the NASA EVA 23 water incursion (Hansen, 2013), which indicated it was difficult to define corrective actions for findings that were related to “human nature.” We believe RE can add unique value beyond existing risk management approaches by offering innovative practices to learn, collaborate, prepare for surprise, and notice and respond to the unexpected. Table 4 compares a resilience engineering approach in comparison with traditional risk management.

Table 4: Comparison between Traditional and Resilience Engineering Approaches

Type of finding	*Traditional Risk Management*	*Resilience Engineering*
Share lessons learned from failures “in a way that people take them to heart and can find them faster.”	Document lessons in databases. Require staff to periodically read and study.	Learn from what goes well. Find similar events where things went well, ask “*why* did this go well?”
Informal pressure and deference to rank inhibit speaking up.	Encourage front line workers to speak-up (e.g., “If you see something, say something.”)	Practices that increase speaking up and collaboration: change format of meetings such that leaders speak last, round robin, train leaders to ask open ended questions, invite cross-checks, leave rank at the door.
Failure in responding to unexpected situation.	Create rules to specify expected response.	Develop drill and simulation scenarios that include surprising branches, subtle cues. Assess how collaboration, social influences, affect response to weak signals.

4. **CONCLUSIONS**

Resilience engineering enables those who study and work in complex high risk settings such as the ISS to become sensitive to, and manage, potential threats to mission success. The Resilience Analysis Grid offers an efficient, accessible means to study complex socio-technical systems, supporting both quantitative and qualitative inquiry. The RAG is simple, accessible, and gets at the true nature of the system under consideration. At the same time, its simplicity makes it necessary for those who are new to the method to learn more about how to use it. Thematic analysis of data using the RAG will benefit from the use of software that has been developed for this purpose. Those who use the RAG in the future, particularly those who are new to the method, may benefit from interactive orientation and training such as case studies, drills and simulation.

Acknowledgements

The work reported in this paper was funded by the NASA Engineering and Safety Center.

REFERENCES

Aaen-Stockdale, C. (2014). Oil and gas, technology and humans: assessing the human factors of technological change. Ergonomics, 57(6), 956-957.

CAIB. (2003, August). *Columbia Accident Investigation Board Report*. National Aeronautics and Space Administration. Washington DC.

Hansen, C. (2016, June). Chair, EVA Mishap Investigation Board. NASA Project Management/Systems Engineering (PMSE) Forum. Retrieved 1 September 2016, from http://www.ustream.tv/ recorded/88356593.

Hollnagel, E. (2012). *FRAM : The Functional Resonance Analysis Method*. Farnham, UK : Ashgate Publishing.

Hollnagel, E. (2011). RAG – The Resilience Analysis Grid. In: E. Hollnagel, J. Pariès, D. D.Woods & J. Wreathall (Eds). *Resilience Engineering in Practice. A Guidebook*. Farnham, UK: Ashgate.

Ljunberg, D. & Lundh, V. (2013). Resilience Engineering within ATM - Development, adaption, and application of the Resilience Analysis Grid (RAG). University of Linköping, LiU-ITN-TEK-G--013/080--SE.

Mishap Investigation Board (2013, December). International Space Station (ISS) EVA Suit Water Intrusion High Visibility Close Call. IRIS Case Number: S–2013–199–00005. Johnson Space Center. National Aeronautics and Space Administration. Houston, TX.

NASA (2017). *The International Space Station (STS-129 Crew, Expedition 21 Crew).* Retrieved on 5 May 2017 from the NASA Astronomy Picture of the Day 2009 Dec 7th web site, https://apod.nasa.gov/apod/ ap091207.html

Nemeth, C. & Herrera, I. (2015). Preface: Building change- Resilience engineering at ten years. In C. Nemeth & I. Herrera (Eds.). Special issue on Resilience Engineering. *Reliability Engineering and System Safety*. 141. http://dx.doi.org/ 10.1016/ j.ress.2015.04.006.

Orasanu, J., Martin, L. & Davison, J. (2001) Cognitive and Contextual Factors in Aviation Accidents: Decision Errors. In E. Salas and G. A. Klein (Eds.), *Linking Expertise and Naturalistic Decision Making*. Mahwah, New Jersey: Lawrence Erlbaum, 209-225.

Rogers Report. (1986, 6 June). *Report to the President By the Presidential Commission On the Space Shuttle Challenger Accident.* National Aeronautics and Space Administration. Washington DC.

Woods, D.D. (2012). In Leveson, N. (2012). *Resilience Engineering*. Farnham, UK: Ashgate Publishing. Retrieved from http://www.ebrary.com. Created from linkoping-ebooks on 2016-09-23 00:45:48.

INNOVATION RESILIENCE IN TEAM WORK: ANTECEDENTS AND RESULTS FROM A STUDY OF INNOVATION TEAMS IN THE NETHERLANDS

Peter R.A. Oeij [1 2]

[1] TNO, Schipholweg 77-89, 2316 ZL Leiden, The Netherlands

[2] Open University of The Netherlands, Valkenburgerweg 177, 6419 AT Heerlen, The Netherlands

[1 2] peter.oeij@tno.nl

http://www.tno.nl

Abstract

Organising in a mindful way is key to helping innovation teams become more resilient and thereby increase the chances of innovation success. Organising as such, called mindful infrastructure, implies creating the right conditions for teams to excel. To this end, four elements are crucial. When teams are 1) feeling psychologically safe, 2) experience a learning environment, 3) have a say in decision-making, and 4) see that leadership creates synergy, the foundation is laid for resilient team behaviour. In turn, this team innovation resilience behaviour enables teams to successfully deal with critical incidents, which, otherwise, could lead to innovation failure. Resilient innovation teams are extremely alert to small things that can become big problems, hate to jump to conclusions, link management goals with operational practice, value expertise stronger than rank, and can radically change course if required. This helps them keep their innovation projects on track and thus improve the chances of innovation success. This study first transfers insights of crisis and safety management to that of innovation management; second, it has sought to investigate the scientific underpinnings of mindful infrastructure and team innovation resilience behaviour. Third, it provides practical guidelines for building a Resilient Innovation Team.

INTRODUCTION

Innovation as a team process is the human effort in teams to develop, support and implement the renewal and improvement of a product, a service or a process (Oeij, 2017). An important question is why projects and innovations often fail. Failure rates of innovation projects are high. Castellion and Markham (2013) report a failure rate of 40% of product innovations. The problem statement of this study is that the substantial failure rates of projects and innovations is a big expense for both companies and society.

Shenhar and Dvir (2007) argue that most people believe projects fail due to poor planning, a lack of communication, or inadequate re-sources, but the evidence suggests that failure is often found even in well-managed projects run by experienced managers and supported by highly regarded organisations. Projects are strongly affected by well-known 'hard' factors, but also by less known 'soft' factors. Being able to adjust a project requires a shift of attention from only the 'hard factors' to including the 'soft factors'. Hard factors, such as the project management's iron triangle - the triple constraint of the criteria to complete the project on time, within budget and within performance goals or requirements - remain important, but soft factors, such as behaviour, leadership, skills, communication, and organisational culture, should not be ignored. The complexity of projects, where the small details of projects are inherently unpredictable, which can have serious consequences, is more often caused by people, than by a product or process (Azim, Gale, Lawlor-Wright, Kirkham, et al., 2010). Team behaviour and the environment of teams therefore contain crucial leverage factors for both failure and success.

The research objective is to find out how project teams can improve their innovation processes. As the focus is on team behaviour in this study, the research asks how team members deal with the fact that innovation projects might be complex, and that risk-averse behaviour may be involved in the failure of innovation projects. The innovation process in a project might be negatively affected by complex experiences that could trigger defensive behaviours (Cicmil & Marshal, 2005). As a consequence, team members become risk-averse, make defensive responses (Argyris, 1990), and the innovation project might be threatened. Our purpose is to investigate the conditions under which such innovation teams can perform better.

For this purpose the study used insights from the crisis management and safety literature of High Reliability Organisations (Tolk, Cantu & Beruvides, 2015). These organisations proved able to perform without major accidents while working under high pressure. What characterises these organisations is that they have developed a high level of awareness of possible mistakes, and the ability to deal with mistakes in the event that they might occur, which they call 'collective mindfulness'. On the basis of this awareness their teams are able to function very effectively; they excel in anticipating and preventing risky situations that might escalate, and if such risky situations emerge nonetheless, those teams are able to contain the risks, get back on track, and keep the system functioning and performing under pressure. High Reliability Organisations (HROs) have developed organisational environments that encourage trust, and openness, and extremely high motivation and psychological effort to eradicate mistakes and the possible causes of mistakes. HROs invest heavily in organisational learning, and in combining rules and procedures with modes of high adaptivity, and being able to manage the unexpected (Weick & Sutcliffe, 2007). Two concepts are derived and modified from the crisis management and safety literature which we call 'mindful infrastructure' and 'innovation resilience behaviour'. Mindful infrastructure involves the organisational facilitation of effective team work; innovation resilience behaviour is the team behaviour itself, which is built on five principles that ensure it is effective (Oeij, 2017).

The line of reasoning in the study is, that by applying the principles of HROs, it is expected that teams can successfully deal with critical incidents during their innovation projects. Critical incidents (Flanagan, 1954) are situations or events that threaten the successful process of an innovation project. The ability of the teams applying the HRO-principles means that they can solve critical incidents and even prevent them from occurring, or from escalating once they emerge (Alliger, Cerasoli, Tannen¬baum & Vessey, 2015). Such team behaviour can only be expected if teams are embedded in a team environment that enables this kind of behaviour when performing in complex projects (Vidal & Marle, 2008). Such project teams, for instance, must ensure that they are creative, and at the same time cost-effective. In such seemingly incompatible instances it might be tempting to achieve only the goals for which the team is held accountable, and that are tangible. Being cost-effective is perhaps more tangible and accountable, and psychologically less effort (Kahneman, 2011) than being creative, but is to the detriment of the innovation goals of a project. Serving ambiguous goals is difficult and conducive to defensive risk avoidance (Argyris, 1990), which is to be avoided in innovation teams. This study therefore explores the aspects of a team environment that enable what we call 'innovation resilience behaviour'. The term we use for this kind of organisational facilitation is 'mindful infrastructure'. We assume that what HRO-teams can do, could also be beneficial for non-HROs, in order to reduce the failure rate of projects and innovations in project teams. The main question of the study is: How do project teams deal with critical incidents during their innovation projects?

THE RESEARCH FRAMEWORK AND RESEULTS

Theoretical Framework

The study (Oeij, 2017) is rooted in the author's fascination about why so many innovations seem to fail. The researcher's curiosity was driven by initial questions such as: do innovation projects fail because such projects are complex (Geraldi, Maylor & Williams, 2011; Vidal & Marle, 2008)? Do they fail because people in teams become defensive when there is tension, uncertainty and fear (Cicmil & Marshal, 2005)? Somewhere, outside the world of innovation management, there are teams -HRO-teams- that hardly ever fail. These are teams working in high-risk situations, namely teams in nuclear plants, on aircraft-carriers, in operating rooms, and in fire-brigades. Why do such teams hardly ever fail (Cantu et al., 2015; Hollnagel, 2006; Righi, Saurin & Wachs, 2015; Weick & Sutcliffe, 2007)? Moreover, can innovation teams learn from HRO-teams? What basically characterises HRO-teams is summarised in Figure 1: they are embedded in an organisational context that nourishes trust, learning, commitment and supportive leadership: a mindful infrastructure. Due to that context, a certain kind of team behaviour is enabled that minimises making mistakes and gets a team back on track should a mistake or accident occur (Oeij, 2017). That type of team behaviour is based on five HRO-principles (Weick & Sutcliffe, 2007; Weick, Sutcliffe & Obstfeld, 1999), namely: 1. Be very alert to things that go wrong or indicate negative consequences; 2. Do not accept simple answers but try to validate the facts; 3. Rule out doubt by unambiguously connecting the broad organisational goal and the team work; 4. Anticipate possible and unexpected failure and ensure resilient responses; 5. Rank expertise higher than hierarchy. We mapped this team behaviour to innovation teams and called it innovation resilience behaviour.

Fig. 1: Mindful infrastructure as enabler of innovation resilience behaviour

HRO-teams are able to minimise accidents and contain their escalation should they nonetheless occur: they have excellent team results. However, team results of innovation teams are different, namely achieving progress and positive results instead of failure of innovations. Therefore, the research is directed at the applicability of HRO-principles in the context of innovation.

To answer the central question how project teams deal with critical incidents during their innovation projects, and what characteristics such teams have, for example whether they are teams embedded in a mindful infrastructure, this study looked into the presence of team psychological safety (Edmondson, 1999; 2012), team learning behaviour (Edmondson, 1999; 2012), team voice (LePine & Van Dyne, 2001) and complexity leadership (Lawrence, Lenk & Quinn, 2009). These are the research variables of the above mentioned trust, learning, commitment and supportive leadership. To investigate if teams subsequently perform innovation resilience behaviour (Team IRB), this study assesses the presence of the five HRO-principles that were modified by team behaviour in innovation teams (Fig. 2).

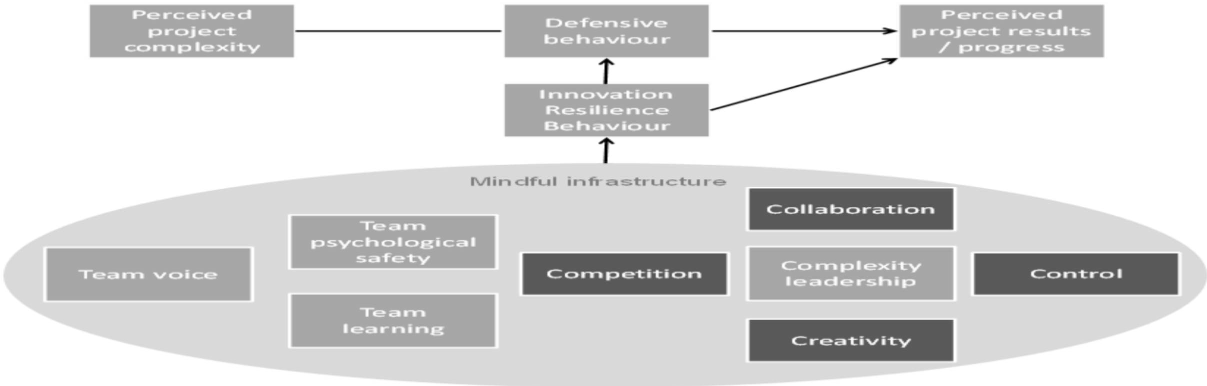


Fig. 2: The theoretical framework of the research.

This study assumes that complexity of projects and defensive behaviour of team members could affect the innovation project in a negative way. A possible cause for defensiveness is project complexity (Cicmil & Marshall, 2005), which refers to unpredictable and unexpected situations that emerge from the interaction of many factors in innovation projects. Talking about complexity (Vidal & Marle, 2008), one can, for example, think about intricate technological and intellectual demands related to the innovation goal, differing interests of stakeholders of the innovation, external influences due to decisions about strategy and finance, priorities taken by others outside the team, and team conflict. If project complexity induces defensive behaviour, then perhaps the presence of mindful infrastructure and IRB could keep the team and the project on track, in order to still achieve a desired outcome (the perceived project results or progress). IRB can also directly lead to good project outcomes (Fig. 2). The main question is divided into seven research questions: 1] What is mindful infrastructure and what is Team IRB? What is their relationship?; 2] Does IRB affect perceived project results and perceived project progress?; 3] Do teams have different configurations of mindful infrastructure?; 4] Is IRB associated with defensive behaviours?; 5] How do project leaders manage innovation projects?; 6] How do teams respond to critical incidents during innovation projects?; 7] What can innovation management teams learn from HRO teams?

Methodology

The research took place among eleven Netherlands-based organisations, some of them are multi-nationals. These organisations are selected from the manufacturing sector, services and education; some are profit organisations, others are non-profit organisations. In these eleven organisations, eighteen teams and their innovation projects are studied as cases studies, and additionally team members working in similar projects in those companies participated in a survey (309 respondents). A pilot study preceding the main study was executed in a Dutch research and technology organisation.

A case study approach was chosen as the main approach to gather information. In each case we held face-to-face and group interviews with team leaders, team members and the project manager. We approached these teams, their managers, and an additional sample of colleagues in their organisation, performing the same kind of project-based innovation projects, with a questionnaire to gather data suitable for statistics. Finally a team was observed during a team meeting. To analyse the data we used quantitative 'correlational' techniques (e.g. multiple regression analyses), quantitative 'configurational' techniques (qualitative comparative analysis), and qualitative techniques (discourse analysis, content analysis). To interpret the results we used deductive reasoning (e.g. the use of the HRO-literature in crisis management and safety in the domain of innovation management) and inductive reasoning (e.g. in making sense of defensive behaviours and reflective leadership we used the theories of organisational defence mechanisms, reflective practitioner model and organisational learning model). This study combines the positivist approach of hypothesis testing using quantitative data with the interpretivist approach of theory building (and hypothesis-generation) from cases with qualitative data (Oeij, 2017: 21-22).

Results of the study

The total investigation consists of six studies. Study 1 is a pilot study of a single case, namely an innovation programme in a research and technology organisation (Oeij, Dhondt, Gaspersz & De Vroome, 2016). Based on this study, the framework model above was developed. The study combines survey data, in-depth face-to-face interviews, and the observation of a project team, and concludes that there are positive associations between team mindfulness, team psychological safety, and team learning behaviour. To the degree that more team mindfulness, team psychological safety, and team learning behaviour are present, there are better project results, in terms of more team innovativeness, and team external and team internal effectiveness. A relation with the type of project (innovation project or regular, non-innovative project) and project complexity was not found.

Study 2 (Oeij, van Vuuren, Dhondt & Gaspersz, 2016) explores the main relations of the model (Fig. 2) based on survey data from innovation teams from eleven companies where project teams are working on innovations (study 2 addresses questions 1 and 2). The elements of mindful infrastructure - team psychological safety, team learning behaviour, team voice and the leadership style control – were associated with Team IRB. Similar to study 1, this study found that perceived project complexity did not influence Team IRB. Further, mindful infrastructure was positively associated with project outcomes (perceived project success and perceived project progress), but this relation was significantly stronger when Team IRB was present at the same time. Team IRB mediated the relationship between mindful infrastructure and project outcomes.

Study 3 investigates patterns of mindful infrastructure (Oeij, Dhondt & Gaspersz, 2016), that is, the presence in teams of combinations of (seven) variables of mindful infrastructure (Fig. 2), so-called 'configurations' (this study addressed question 3). Based on 18 cases of innovation projects of just as many teams, there were eight different combinations of mindful infrastructure variables discovered that have a similar result, as it happens to be that each of those patterns was related to the presence of Team IRB in these teams. This implies that teams can have a different design of mindful infrastructure to achieve Team IRB. However, the eight patterns found suggest that those combinations have a better chance to enable Team IRB than other combinations. With a certain probability it is concluded one should realise that seven variables can lead to 128 possible configurations, thus 120 configurations are not 'true'.

Study 4 investigates defensiveness in teams (and addressed question 4) (Oeij, Dhondt, Gaspersz & Van Vuuren, 2016). Indications were found that teams that were less capable of Team IRB were more inclined to show defensive behaviour, which means these teams were more conducive to try to be in control, to prevent losing control and to avoid feelings of embarrassment. It seems that teams less capable of Team IRB were more risk-avoiding. The study seems to point out that teams capable of Team IRB have more project success. The research also led to the development of an instrument to measure certain defensive behaviours when analysing conversations.

Study 5 researches how project leaders manage their innovation projects (research question 5) (Oeij, Gaspersz, Van Vuuren & Dhondt, 2017). Some project leaders implicitly applied a rigorous research methodology when they have to deal with critical incidents. They followed specific steps: recognise the problem, investigate the problem, develop alternative solutions, test their validity, try out and experiment solutions, select and apply one solution, and evaluate the completed process. Surprisingly these project leaders applied the model of the 'reflective practitioner' developed by Schön (1983, 1987), who contended that experienced professionals use that model tacitly, without being aware of it. Theorising on what we observed, in a subsequent conceptual step, we linked the reflective practitioner model to the control cycle that is part of the organisational learning model (Argyris & Schön, 1996), which integrates single, double and triple loop learning. By making the combined model explicit, assistance was provided for developing ways to train project leaders in becoming more rigorous and resilient whilst learning in leading their innovation projects, and thus reducing the chance of project failure.

Study 6 (Oeij, Dhondt, Gaspersz & Van Vuuren, accepted 2017) explored how teams deal with critical incidents during innovation projects (research question 6). Focusing on the twelve out of eighteen teams that were capable of performing Team IRB, the main finding was that these twelve teams were better at managing and mending critical incidents than in minimising critical incidents. One can say that, unlike HRO teams, who excel in preventing incidents from escalating, the innovation teams capable of Team IRB were more responsive than pro-active, except for those teams embedded in an R&D environment. In these R&D-embedded teams specific project management tools were present, which might explain a more pro-active position and attention toward risk management.

The answer to the question of what innovation management teams can learn from HRO teams (question 7) is found in the HROs' emphasis on the psychology of mindful acting and the organisational discipline to systematically embed organisational routines such as dedicated briefings and debriefings. HROs excel in creating space for learning and speaking up, and to meticulously improve the work process wherever possible, and in so doing test and redesign their routines; their routines never stay the same for long, as they continuously evolve. Paradoxically, HROs are capable of balancing between required rule-based routines and the emerging need to adapt those routines. HROs inform innovation management with its attention toward the psychology of avoiding mistakes and putting effort in unnatural human behaviour. The psychological concepts of reliability and mindfulness, underlying the five HRO-principles, explain the motivation to continuously be aware of unforeseen situations, and ensure continuous learning from events that each time unfold in slightly different ways (Weick & Sutcliffe, 2007). Applying these insights can support the signalling of weak signals of failure by innovation team members and suppress defensive, risk-avoiding behaviour, and therefore ultimately enhance the chance of innovation success.

CONCLUSIONS AND RECOMMENDATIONS

The main conclusion of the study is that, indeed, mindful infrastructure and Team IRB are concepts that can be applied to innovation management and project teams working on innovation. Innovation teams that do apply these insights seem to be less defensive and report positive project outcomes more often. While this insight is instructive to innovation management as a field, the findings also add to the knowledge of safety and crisis management, in the sense that mindful infrastructure consists of the elements of team psychological safety, team learning behaviour, team voice and complexity leadership. These are the antecedents for the HRO-principles already applied (Sutcliffe, Vogus & Dane, 2016).

In terms of recommendations to develop 'The Resilient Innovation Team' the research suggests that mindful infrastructures, that support openness and trust, enable teams to perform Team IRB and be less defensive, are all helpful in making complex issues and uncertainties discussable. Instead of becoming risk-averse such teams are solving the project's risks and critical incidents with openness and effectiveness. Some project leaders deploy a research-driven perspective to solve critical incidents with the kind of transparency and validation of solutions that helps to overcome defensive routines in highly resilient ways. Some project teams, notably those embedded in R&D organisations, are better at preventing and minimising critical incidents than other teams. HRO-teams are still even better at minimising incidents and accidents, which means that for innovation teams much is to be won in this regard. The Resilient Innovation Team is able to proactively handle unexpected, sometimes critical, events to continue pursuing its (project, innovation or team) goal without significant disruption. Practical guidelines and a tool (Oeij, 2017; Oeij, forthcoming 2017) are provided to develop both mindful infrastructure and Team IRB, and to combat defensive behaviour.

REFERENCES

Alliger, G. M., Cerasoli, C. P., Tannenbaum, S. I. & Vessey, W. B. (2015). Team resilience: How teams florish under pressure. *Organizational Dynamics, 44*(3), 176–184.

Argyris, C. (1990). *Overcoming organizational defenses. Facilitating organizational learning*. Upper Saddle River, NJ: Prentice Hall.

Argyris, C. & Schön, D. A. (1996). *Organizational learning II. Theory, method, and practice*. Reading (MA), etc.: Addison-Wesley (2nd ed., 1st ed. 1978).

Azim, S., Gale, A., Lawlor-Wright, T., Kirkham, R., Khan, A. & Alam, M. (2010). The importance of soft skills in complex projects. *International Journal of Managing Projects in Business, 3*(3), 387-401.

Castellion, G. & Markham, S. K. (2013). Perspective: New product failure rates: Influence of argumentum ad populum and self-interest. *Journal of Product Innovation Management, 30*(5), 976–979.

Cicmil, S. & Marshall, D. (2005). Insights into collaboration at the project level: Complexity, social interaction and procurement mechanisms. *Building Research & Information, 33*(6), 523-535.

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, 44*(2), 350-383.

Edmondson, A. C. (2012). *Teaming. How organizations learn, innovate, and compete in the knowledge economy*. San Francisco, CA: Jossey-Bass.

Flanagan, J.C. (1954). The critical incident technique. *Psychological Bulletin, 51*(4), 327-358.

Geraldi, J., Maylor, H. & Williams, T. (2011). Now, let's make it really complex (complicated). A systematic review of the complexities of projects. *International Journal of Operations & Production Management, 31*(9), 966-990.

Hollnagel, E. (2006). Resilience: the challenge of the unstable. In E. Hollnagel, D. D. Woods and N. Leveson (Eds), *Resilience engineering. Concepts and precepts* (pp. 9-17). Aldershot and Burlington: Ashgate.

Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

Lawrence, K. A., Lenk, P. & Quinn, R. E. (2009). Behavioral complexity in leadership: The psychometric properties of a new instrument to measure behavioral repertoire. *The Leadership Quarterly, 20*(2), 87-102.

LePine, J. A. & Van Dyne, L. (2001). Voice and cooperative behavior as contrasting forms of contextual performance: Evidence of differential relationships with Big Five personality characteristics and cognitive ability. *Journal of Applied Psychology, 86*(2), 326-336.

Oeij, P.R.A. (2017). *The resilient innovation team: a study of teams coping with critical incidents during innovation projects*. PhD Dissertation Open University of The Netherlands.

Oeij, P.R.A. (forthcoming 2017). From automated defensive behaviour to innovation resilience behaviour: A tool for resilient teamwork as an example of workplace innovation. In: P.R.A. Oeij, D. Rus & F.D. Pot (Eds). *Workplace Innovation: Theory, Research and Practice*, Volume in 'Aligning Perspectives on Health, Safety and Well-Being' series. Berlin etc.; Springer.

Oeij, P. R. A., Dhondt, S. & Gaspersz, J. B. R. (2016). Mindful infrastructure as an enabler of innovation resilience behaviour in innovation teams. *Team Performance Management: An International Journal, 22*(7/8), 334-353.

Oeij, P. R. A., Dhondt, S., Gaspersz, J. B. R. & De Vroome, E. M. M. (2016). Can teams benefit from using a mindful infrastructure when defensive behaviour threatens complex innovation projects? *International Journal of Project Organisation and Management, 8*(3), 241-258.

Oeij, P.R.A., Dhondt, S., Gaspersz, J.B.R. & Van Vuuren, T. (2016). Defensive behaviours in innovation teams – how project teams discuss defensiveness and its relationship with innovation resilience behaviour and project success. *Language, Discourse & Society*, 4(2), 15-36.

Oeij, P.R.A., Dhondt, S & Gaspersz, J.B.R. & Van Vuuren, T. (accepted 2017). Innovation resilience behaviour and critical incidents: validating the Innovation Resilience Behaviour scale with qualitative data. *Project Management Journal*.

Oeij, P.R.A., Gaspersz, J.B.R., Van Vuuren, T. & Dhondt, S. (2017). Leadership of innovation projects: an illustration of the reflective practitioner and the relation to organisational learning model. *Journal of Innovation and Entrepreneurship*, 6(2), 1-20.

Oeij, P. R. A., Van Vuuren, T., Dhondt, S. & Gaspersz, J. (2016). Mindful infrastructure as antecedent of innovation resilience behaviour of project teams. *IWOT 20 - International Workshop on Team Working*. Open University, Utrecht, 9 September 2016.

Righi, A. W., Saurin, T. A. & Wachs, P. (2015). A systematic literature review of resilience engineering: Research areas and a research agenda proposal. *Reliability Engineering & System Safety, 141*(10), 142-152.

Sauser, B. J., Reilly, R. R. & Shenhar, A. J. (2009). Why projects fail? How contingency theory can provide new insights – A comparative analysis of NASAs Mars Climate Orbiter loss. *International Journal of Project Management, 27*(7), 665-679.

Schön, D. A. (1983). *The reflective practitioner: How professionals think in action*. New York: Basic Books.

Schön, D. A. (1987). *Educating the reflective practitioner. Toward a new design for teaching and learning in the professions*. San Francisco (etc.): Jossey-Bass.

Shenhar, A. J. & Dvir, D. (2007). *Reinventing project management. The diamond approach to successful growth and innovation*. Boston, MA: Harvard Business School Press.

Sutcliffe, K. M., Vogus, T. J., & Dane, E. (2016). Mindfulness in organizations: A cross-level review. *Annual Review of Organizational Psychology and Organizational Behavior*, *3*, 55-81.

Tolk, J. N., Cantu, J. & Beruvides, M. (2015). High Reliability Organization research: A literature review for health care. *Engineering Management Journal, 27*(4), 218-237.

Vidal, L.-A. & Marle, F. (2008). Understanding project complexity: Implications on project management. *Kybernetes, 38*(8), 1094-1110.

Vogus, T. & Iacobucci, D. (2016). Creating highly reliable health care: How reliability-enhancing work practices affect patient safety in hospitals. *Industrial and Labor Relations Review / ILR Review, 69*(4), 911-938.

Weick, K. E. & Sutcliffe, K. M. (2007). *Managing the unexpected. Resilient performance in an age of uncertainty* (2nd ed.; 1st ed. 2001). San Francisco: Jossey-Bass.

Weick, K. E., Sutcliffe, K. M. & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. In: R. S. Sutton and B. M. Staw (Eds.), *Research in Organizational Behavior, 1* (pp. 81–123). Stanford: Jai Press.

PREPARING TO BE UNPREPARED: TRAINING FOR RESILIENCE

David Passenier [1], Daan Pool [2], Amy Rankin [3] and Alexei Sharpanskykh[4]
[1]VU Amsterdam, De Boelenlaan 1081, 1081 HV Amsterdam, The Netherlands
[1]d.f.passenier@vu.nl
[2, 4]TU Delft, Aerospace Engineering, Kluyverweg 1, 2629 HS Delft, the Netherlands
[2]d.m.pool@tudelft.nl
[4]o.a.sharpanskykh@tudelft.nl
[3]Department of Computer and Information Science, Linköping University, Sweden
[3]amy.rankin@liu.se +4613282757

Abstract

Training methods for operators working under high pressure and in dynamic, unpredictable settings could benefit from a focus on resilience. In such settings, formal training often focuses on procedural conformity to train for particular scenarios, but resilient performance taps into a wider experience base and often more tacit skills. In this paper, we formulate a research agenda to develop useful theoretical insights about training for resilience. Our discussion follows recent developments on organizational routines, which suggest that sources of inertia and conformity, such as strict procedural training, can also enable operators' resourcefulness. Drawing from our diverse research experiences, we discuss the training needs for 1) developing or attenuating techniques for flexible procedural use, grounded in a rich qualitative understanding of practical experience; 2) the possibility to train skills that are more broadly applicable than specific training scenarios through simulation training methods; and 3) the development of training programs based on knowledge of "work-as-done" through Agent Based Modelling and Simulation methodologies and behavioral theories.

INTRODUCTION

Practical knowledge and experience are increasingly regarded as crucial facets of operational resilience (Weick & Sutcliffe, 2011). Resilience matters in conditions where operators work under high pressure in dynamic and unpredictable settings, facing major consequences if something goes wrong. Operators working in such conditions build knowledge and experience by learning in formal training, participating in communities of practice, and internalizing lessons from on-the-job performance. Knowledge and experience thus gained, often tacitly, can make operators resourceful and enable them to act adequately in surprising and ambiguous situations.

Formal training provides important building blocks to operate resiliently, but does not necessarily ensure management of unexpected events when instructions are only about following procedures. Procedures are useful guidelines in ambiguous, complex situations when operators know when, how, and why to deviate. This raises questions about what training for resilience would look like. What type of training could access and stimulate experiential learning and informally acquired knowledge? For what kind of situations could or should operational personnel be prepared to deviate—emergencies, routine situations, or both? Could or should formal training simulate the real world better?

In this paper, we formulate a research agenda to develop useful theoretical and methodological insights about training for resilience. To this end we first identify and elaborate on the challenges that exist in training for resilience. We draw from our diverse research experiences to outline topics of interests, methodological challenges, and contributions with the potential to quickly update current training practices. Consistent with organizational routines literature (e.g. Grote, Weichbrodt, Günter, Zala-Mezö & Künzle, 2009), we find that training can stimulate conformity, which helps to establish predictability and reliability, but conformity does not necessarily contribute to resilience. Training for resilience taps into, acknowledges and supports the variability of routine performance. Managing variability better may require training a different skill set than those associated with creating conformity to procedures. Furthermore, to establish how training of resilient skills translates to its practical application, we may need to develop alternative methodologies that can capture the variable nature of operational work as done.

Our discussion on resilience training challenges is guided by three, interrelated questions. First, we develop a theoretical perspective on flexible versus robust procedures. How can operators be guided to know when to deviate from normal procedure? Second, we review the training of broadly applicable skills that allow for coping with unexpected and untrained scenarios. Can general problem-solving skills provide a useful baseline to adapt to unexpected events? Third, we discuss ways to develop training programs based on knowledge of "work-as-done". How can knowledge about everyday challenges and adaptive performance inform training scenarios? We conclude our paper with a broad research agenda that can address these questions in relation to one another.

RESILIENCE CHALLENGES

2.1 Flexible vs robust procedures

Organizational rigidity and inertia are often seen as obstacles to the adaptive behaviors required for resilient performance (Weick & Sutcliffe, 2011). Normative management policies that focus on controlling behaviors, such as by enforcing compliance with procedures, are effective in limited degrees, because while some situations require robust procedures, others require flexibility (Hale & Borys, 2013). Recent developments in organizational sciences however suggest that commonly acknowledged sources of inertia and rigidity, such as robust procedures, may also function as sources for improvisational resourcefulness (Levental & Rerup, 2006).

Organizational routines are a useful unit of analysis to understand how deviating can be normal without endangering, but rather sustaining the continuity of an operation (Pentland & Feldman, 2005). Organizational routines conceptually represent the common sense-understanding of organizational continuity through repetition and habit, while also acknowledging that every single performance of a routine varies with respect to the one before. Furthermore, complex routine dynamics can be found in the shifting ways in which organizations standardize their routines, attempt to create conformity in routine performance, or leave more to professional discretion. This insight could be translated as designing additional, flexible procedures to handle non-normal situations. Alternatively, organizations could acknowledge the flexibility of existing procedures and train operators to motivate deviations and exercise professional discretion.

One application of the organizational routines perspective is to design organizational routines with its inherent flexibility in mind (Grote et al., 2009). A good example is a recent study to create flexible procedures for flight crews. Modern flight crews operate in an environment with multiple detailed procedures to cover abnormal events. Complex and unexpected events without a clear procedure or systems solution are rare, and may thus present a challenge to the crew in knowing how to assess the situation and decide on a course of action. In a recent simulator study of flight crew's ability to respond to unexpected events, a procedure was developed that would assist crews in responding to events with situations where no single procedure was applicable and thus required a certain amount of problem solving and decision making (Field, Rankin, Mohrmann, Boland & Woltjer, 2017). The procedure offers a set of high-level strategies on the topics of problem solving, decision making, leadership and communication for responding to an event where there is no single and clear procedure. The procedure further has three focus areas: managing time criticality, managing (un)certainty, and to plan for contingencies and changes.

Another, similar approach, could be to acknowledge that existing procedures are to some degree flexible. Training then implies offering a range of high-level techniques—many of which are already being taught—to enact procedures in improvisational action trajectories. In aviation, pilots for example learn that the immediate response to a sudden disturbance is 'aviate, navigate, communicate'. These techniques help diagnose and structure an ambiguous situation and are often informally included in training, relying more on pilots' personal career experience. In an interview study (Passenier, de Bakker, Groenewegen, Wolbers & Catz, 2016), for example, a Dutch pilot explained what 'pro-active improvisation' by referring to a risk management technique used in German airlines. Improvisational action trajectories can refer to a broad range of situations and include any alteration of normal, routine, or prescribed techniques to conduct the operation, such as by creative reordering of steps, mixing procedures or techniques, or cropping checklists to suit the circumstances. Training operators to handle the array of robust to flexible procedures, prompts the following questions:

- How can high level procedures or techniques be defined?
- What kind of skills do operators need to apply procedures in ambiguous settings?
- How can organizations make the most of individual differences of learners?
- How can the organizational (training) culture facilitate flexible uses of procedures?

By investigating these questions, training can begin to tap into the experiential knowledge base of operators and link these with the development of skills that contribute to resilient performance.

2.2 Training general problem skills

The key to success in coping with unexpected events in many industries today still lies with the decision-making, supervisory control, or manual control skills of (teams of) individuals. Still, most current training programs – for example in aviation – mostly focus on pre-defined skills and context-specific scenarios where trainees know what to expect. The focus is on anticipating and mitigating variations, faults and failures at a system level and flight crews have little exposure to truly unexpected events (Advani, Schroeder & Burks, 2010; Casner, Geven, &

Williams, 2013). Recent experiments on aerodynamic stall recovery training have shown that pilots confronted with abnormal events in the context of a well-known training scenario quickly recognised and carried out the appropriate responses (Casner et al., 2013). However, when presented with similar events but with different timing and in a different context, they failed to recognise and recall the appropriate response (Casner et al., 2013; Schroeder et al., 2014), implying that responses learned and practiced during current airline training may not be generalizable to more naturalistic settings. Creating such truly naturalistic settings, with realistic surprise, in training programs (and thus *repeatedly*) is impractical, if not impossible (Advani et al, 2010). Possible solutions, such as scenario-based training, require instructors that are highly skilled at deception of their trainees and unacceptably increase required training times and thus costs. Therefore, the skills to deal with the unexpected and to "be prepared to be unprepared" in cockpit operations are today largely left to mature through experience.

With persisting incidents and accidents involving unexpected events, aviation authorities, airlines, and pilots themselves have all questioned the effectiveness of this current approach to training for the unexpected. For example, a recent interview study has investigated pilots' experiences with the re-framing process of coping with unexpected events in the cockpit (Rankin et al., 2016; Rankin, Woltjer, Field, & Woods, 2013). The results show difficulties that pilots have in re-framing following a surprising event, including the identification of subtle cues and managing uncertainties regarding automated systems, coping with multiple goals, tasks, narrow time frames, and identifying an appropriate action. The findings of the study suggest that the underlying training issue to cope with surprise is to understand and support the complex socio-cognitive process (Chow, Christoffersen & Woods, 2000) by which pilot's frame and re-frame data based on their knowledge and available cues or triggers. These findings are further supported in recent study of common causes on automation surprises (de Boer & Dekker, 2017), demonstrating that the most common reason for surprise is an incorrect understanding for the automated systems. In this view, training should focus on the process by which pilots search for data, identify relevant cues, manage uncertainties, make trade-offs, re-frame, and decide on a course of action. This can be compared to current training programs focused on e.g., specific competencies or specific known problems (Klein, Woods, Klein, & Perry, 2016).

Two recent studies on role-improvisation in teams responding to a crisis situation (Lundberg & Rankin, 2014; Rankin, Dahlbäck, & Lundberg, 2013) further underline the necessity for direct attention to surprise, sensemaking, and (re-)framing in training. Crisis situations are often characterised by ambiguous and unplanned for events and the need for improvised roles can therefore be of great importance to successfully cope with a crisis. A study of crisis responders in operations following the Tsunami in 2004 and the Lebanon crisis in 2006 (Lundberg & Rankin, 2014) showed that role-improvisation is an important part of crisis response work to cope with dynamic and unpredictable environments. The participants in the study mentioned positive and negative aspects of using role flexibility such as: completing tasks despite a lack of resources, positive team-building effect and increased endurance of the team, decreased efficiency and increased workload due to unclear organisational structure and ineffective planning, increased burden for all team members as people in new roles require more guidance and, people may get stuck in temporary roles. A follow-up study with crisis responders was designed to create a dynamic and non-routine situation in which the participants would be forced to take on roles outside their field of competence (Rankin, Dahlbäck, & Lundberg, 2013). The results showed that improvising in the face of unexpected events is not an ad-hoc activity, but requires training and a strong organisation.

Thus, the importance of exposing trainees to sufficiently surprising, varied and naturalistic training scenarios, to ensure activation of the needed skills during training for a range of potential scenarios, is evident. However, the main challenge lies in how to achieve this without unacceptably increasing training times and costs. Especially since most critical unexpected scenarios are thankfully rare in occurrence, increasing the duration and cost of training is simply not acceptable. In short, what is needed to ensure resilience at the individual human level, is time-efficient training that teaches broadly applicable – generalizable (Healy & Bourne, 2012) – skills that can be proven to transfer from a (limited) training program to untrained scenarios in the real world, which in our view requires addressing the following issues:

- How much variation and truly unexpected scenarios need to be incorporated in a training program to ensure sufficient resilience and an ability to cope with a sufficiently wide range of potential scenarios?
- How could training programs be re-defined to best facilitate training for unexpected scenarios, and with realistic surprise?
- How can advanced training techniques, such as "augmented (reality) training", help reduce training times, keep costs down, and provide trainees with more broadly applicable skills? Augmented training uses virtual training environments to actively emphasize critical task constraints and accelerate the development of an awareness of what information should guide problem solving. Especially in initial (*ab initio*) training (Healy & Bourne, 2012), augmented training has proven potential to reduce training times and instil generalizable

skills that transfer to reality and scenarios different from those used for training (Healy & Bourne, 2012; Ravesteijn, Borst, Pool, van Paassen & Mulder, in prep).

- How can the effectiveness of updated training practices for increasing resilience at the system level be quantified and proven?

In our view, the answers to these questions will increase our understanding of how to actively train for the generalizable recognition, decision, and control skills that will increase resilience at the individual human level. Thereby, these answers will provide the insight needed to make structural improvements to current training programs and ensure trainees are better "prepared to be unprepared".

2.3 Develop training programs based on knowledge of "work-as-done"

Coping with complexity and uncertainty in socio-technical systems requires people to continuously adapt, "fill in the gaps" and find alternative solutions to complete tasks. Although informally recognised by many, the abilities to adapt are not well understood in organisations, leaving a gap of knowledge between "work-as-imagined" and "work-as-done" (Hollnagel, 2014). Knowledge about what enables and disables abilities to successfully adapt to unexpected events is rarely addressed in e.g., accident and incident investigations today, providing a potentially skewed baseline for interpreting actions leading to unsuccessful outcomes. This may further affect assumptions about what is required in terms of training. For example, in a study of crisis response teams (Lundberg & Rankin, 2014; Rankin, Dahlbäck & Lundberg, 2013) the fine balance between situations with successful and less successful outcome are demonstrated, showing how minor details may greatly affect the overall result. This result underlines the argument that successes and failures are closely related (Hollnagel, 2014), and problems that may occur if situations are analysed in hindsight, where the aim is to identify causes of a known outcome. By studying the complexity of everyday events "work-as-done" can inform training design by identifying the cognitive demands of operators in today's complex systems.

Computational social simulation studies based on formal models is a way to investigate "work-as-done" in the context of various operations. Existing formal and computational models of operations in critical infrastructures, particularly in transport and logistics, are predominantly based on the operations research (OR) modelling paradigm (Jensen & Bard, 2003). One of the central challenges in OR-based models and approaches is related to calculating global optima and equilibria states of simplified mathematical representations of operations. Such representations are often based on formal procedures and have limited flexibility. It has been shown that applying such an approach to complex sociotechnical systems, which are in fact complex dynamic co-evolving systems, has a number of issues (Helbing, 2012; Mitleton-Kelly, 2013). Such systems are characterized by the behavior far from equilibria, highly non-linear dynamics, and continuous co-adaptation of different system actors and components. Classical optimization approaches are not necessarily appropriate to such systems, as their state space and, consequently, equilibria and optima are constantly changing.

To address this challenge, more dynamic, adaptive, and agile approaches are needed. As was identified previously (see e.g., Ouyang, 2014, and Mitleton-Kelly, 2013), agent-based modelling and simulation (ABMS) and complex networks paradigms appear to be the most promising to address issues of formal and computational modelling and analysis of complex co-evolving sociotechnical systems. In particular, in previous studies using ABMS it was explored how safety culture emerges from everyday operations, organizational processes, and structures at an air navigation service provider (Sharpanskykh and Stroeve, 2011) and at an aircraft maintenance organization (Passenier, Mols, Bím & Sharpanskykh, 2016). Safety culture was characterized by a set of indicators, dynamic patterns, and trends that emerged from local dynamics and diverse interaction properties of organizational actors and the environment.

A particular focus of the ABMS paradigm is on studying emergence. Often the challenge of understanding emergence takes the form of establishing relations between the local dynamics of agents and global or systemic emergent phenomena. Another example in which this challenge was considered is a recent study of compliance with safety regulations at an airline ground service organization (Sharpanskykh and Haest, 2016). In this study a formal agent-based model was proposed, which explored the role of motivation for (lack of) compliance at the individual, team, and organizational levels. The model was able to reproduce and predict behavioural patterns related to compliance of the platform employees emerging at the organization under study.

One of the central questions that arise in the process of agent-based modelling of sociotechnical systems is how to use and incorporate rich conceptual theoretical basis from behavioral sciences in formal models of multiagent systems. Many of evidences and theories from behavioral sciences are fragmented, informal, high level and sensitive to a specific context. Furthermore, theories may be based on conflicting or inconsistent principles or philosophical viewpoints. This makes integration of different theories in rich sociotechnical system models problematic. We argue that a new generation of modelling techniques to better understand "work-as-done" needs to be developed, taking into account the following issues:

- how could both quantitative and qualitative knowledge of different levels of abstraction from behavioral sciences be used in agent-based modelling and analysis?
- How could ABMS analysis of complex, subtle variation in performance of routine (i.e. repetitive) action patterns distinguish which 'weak signals' (Weick & Sutcliffe, 2011) indicate failure and require active problem solving, and which ones can be ignored?
- How do organizational training routines—e.g. recurrent training cycles—interact with operational routines, such as flying from A to B, responding to an emergency, etc.?

Answering these questions could further our understanding as well as provide more adequate formal models for resilience than currently available. ABMS-based research strategy could also prove to offer good synergy with evidence-based training developments such as in the aviation industry. The ABMS methodology could help articulate a convincing, formal basis for advanced resilience training policies that deviate from the existing training regulations or conventions that might lag behind on these advanced insights.

RESEARCH AGENDA

In this paper, we addressed training needs of operators working under high pressure in dynamic and unpredictable settings, where formal training could prepare operators better for resilient performance. We therefore raised questions about what training for resilience would look like. In the table below, we summarize this research agenda organized by questions about operational variability, the skills needed to handle variability, and methodological development needed to assert these training needs.

Table 8. *Research agenda to train for resilience*

Procedural flexibility	Widely applicable skills	Building on work-as-done
How can operators be guided to deviate from procedures?	How much variability is needed in training secnarios?	How do training routines interact with operational routines?
What kind of skills do operators need to improvise well?	What skills could be generalisable across real work settings?	Which emergent dynamics require problem solving?
How can high-level procedures or techniques be defined?	How can generalised skill training effects be proven?	How can ABMS research use behavioural theories relevant to operator resilience?

REFERENCES

Advani, S., Schroeder, J., & Burks, B. (2010). What Really Can Be Done in Simulation to Improve Upset Training? *AIAA Modeling and Simulation Technologies Conference* (p. 7791).

de Boer, R. J., & Dekker, S. W. (2017). Models of Automation Surprise: Results of a Field Survey in Aviation. *www.preprints.org* accessed on 15-07-2017.

Casner, S. M., Geven, R. W., & Williams, K. T. (2013). The effectiveness of airline pilot training for abnormal events. *Human factors*, *55*(3), 477-485.

Chow, R. Christoffersen, K. & Woods, D.D. (2000). A model of communication in support of distributed anomaly response and replanning. *Proceedings of the 44nd Annual Meeting of the Human Factors and Ergonomics Society/IEA2000, July, 2000.*

Field, J., Rankin, A., Mohrmann, F., Boland, E., & Woltjer, R. (2017). Flexible Procedures to deal with Complex Unexpected Events in the Cockpit. *In: Proceedings of the 7th Resilience Engineering Symposium, Liege, Belgium.*

Grote, G., Weichbrodt, J. C., Günter, H., Zala-Mezö, E., & Künzle, B. (2009). Coordination in high-risk organizations: the need for flexible routines. *Cognition, technology & work, 11*(1), 17-27.

Hale, A., & Borys, D. (2013). Working to rule, or working safely? Part 1: A state of the art review. *Safety Science*, *55*, 207-221.

Healy, A. F., & Bourne Jr, L. E. (Eds.). (2012). *Training cognition: Optimizing efficiency, durability, and generalizability*. Psychology Press.

Helbing, D. (2012). Agent-based modeling. In *Social self-organization* (pp. 25-70). Springer Berlin Heidelberg.

Hollnagel, E. (2014). *Safety-I and safety–II: the past and future of safety management*. Ashgate Publishing, Ltd.

Jensen, P.A. & Bard, J.F. (2003). *Operations research models and methods.* John Wiley & Sons Incorporated.

Klein, D.E., Woods, D.D., Klein, G. & Perry, S.J. (2016). Can we trust best practices? Six cognitive challenges of evidence-based approaches. *J Cogn Eng Decis Making, 10*(3): 244–254.

Levinthal, D., & Rerup, C. (2006). Crossing an apparent chasm: Bridging mindful and less-mindful perspectives on organizational learning. *Organization Science*, *17*(4), 502-513.

Lundberg, J., & Rankin, A. (2014). Resilience and vulnerability of small flexible crisis response teams: implications for training and preparation. *Cognition, technology & work*, *16*(2), 143-155.

Mitleton-Kelly, E. (Ed.) (2013). *Co-evolution of Intelligent Socio-technical Systems. Modelling and Applications in Large Scale Emergency and Transport Domains.* London: Springer.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering & System safety*, *121*, 43-60.

Passenier, D. F., de Bakker, F. G., Groenewegen, P., Wolbers, J., & Catz, E. (2016). Up in the Air: The Construction and Management of Risk by Commercial Airline Pilots. In *Academy of Management Proceedings* (Vol. 2016, No. 1, p. 17488). Academy of Management.

Passenier, D., Mols, C., Bím, J., & Sharpanskykh, A. (2016). Modeling safety culture as a socially emergent phenomenon: a case study in aircraft maintenance. *Computational and Mathematical Organization Theory*, *22*(4), 487-520.

Pentland, B. T., & Feldman, M. S. (2005). Organizational routines as a unit of analysis. *Industrial and corporate change*, *14*(5), 793-815.

Rankin, A., Dahlbäck, N., & Lundberg, J. (2013). A case study of factor influencing role improvisation in crisis response teams. *Cognition, technology & work*, *15*(1), 79-93.

Rankin, A., Woltjer, R., & Field, J. (2016). Sensemaking following surprise in the cockpit—a re-framing problem. *Cognition, Technology & Work*, *18*(4), 623-642.

Rankin, A., Woltjer, R., Field, J., & Woods, D. (2013). “Staying ahead of the aircraft” and Managing Surprise in Modern Airliners. In *5th Resilience Engineering Symposium: Mangaging trade-offs, 25-27 June 2013, Soesterberg, The Netherlands*.

Ravesteijn, C., Borst, C., Pool, D. M., van Paassen, M. M., & Mulder, M. (In prep.). Visually Augmented Simulator-Based Training of the Manual Landing Flare. *IEEE Transactions on Human-Machine Systems*.

Sharpanskykh, A., & Haest, R. (2016). An agent-based model to study compliance with safety regulations at an airline ground service organization. *Applied Intelligence*, *45*(3), 881-903.

Sharpanskykh, A., & Stroeve, S. H. (2011). An agent-based approach for structured modeling, analysis and improvement of safety culture. *Computational and Mathematical Organization Theory*, *17*(1), 77-117.

Weick, K. E., & Sutcliffe, K. M. (2011). *Managing the unexpected: Resilient performance in an age of uncertainty* (Vol. 8). John Wiley & Sons.

FRAM TO ASSESS PERFORMANCE VARIABILITY IN EVERYDAY WORK: FUNCTIONAL RESONANCE IN THE RAILWAY DOMAIN

Patriarca R., Di Gravio G., Costantino F., Tronci M.
Department of Mechanical and Aerospace Engineering,
Sapienza University of Rome
Via Eudossiana 18 - 00184, Rome (Italy)
corresponding author: riccardo.patriarca@uniroma1.it

Abstract

This paper shows the possibility of enhancing the traditional FRAM structure by a semi-quantitative framework in order to increase FRAM's applicability for the analysis of complex systems. This innovative framework consists of defining numeric scores for variability, quantifying in a particular scenario the effects of interactions among functions. Rather than static and deterministic values, it assigns probability distribution functions to the scores, combining them by the aid of Monte Carlo simulation. The distributions, based on Subject Matter Experts' judgments and historic data, if available, allow obtaining an estimation of performance variability and its subsequent functional resonant effects. This semi-quantitative framework allows isolating the critical functions and the critical links among functions, considering non-linear and transient interdependencies. This paper explores the possibility of combining the Monte Carlo framework with an Abstraction/Agency framework recently introduced in literature, in order to make more evident and readable the model itself, maintaining a systemic functional perspective. Once addressed the criticalities and related them to different abstraction levels, it would be possible to plan for mitigating actions. The illustrative case study takes advantage of SMEs and several accident reports in the railway domain to illustrate the application of the proposed semi-quantitative multi-layer framework.

1 INTRODUCTION

In terms of risk and safety management, an interest in human factors became increasingly relevant late in 1980s, to cope with "new" types of accidents, such as the one at Three Mile Island (Hollnagel, Leonhardt, Licu, & Shorrock, 2013). A cause-effect perspective guided the development of methods and model, generally focused at identifying the best fixing strategy for those components most subject to a failure. Following the disasters of Challenger and Chernobyl, both in 1986, it appeared necessary to extend a risk and safety analysis taking into account organizational factors (Vaughan, 1996), (e.g.) adopting the well-established Probability Risk Assessment (PRA) (Stamatelatos, 2002).

In the last two decades, the acknowledgment of systems' complexity started acquiring interest in safety and risk analysis, being concerned with complex system failures and underlying socio-technical factors. Socio-technical systems imply both dual focus and joint optimization of two inter-related sub-systems: the social and the technical system (Pasmore, Francis, & Haldeman, 1982). Technological artefacts interact with individuals, groups, procedures, and even the whole organization, affecting everyday and long-term activities. Those non-negligible tight interactions imply the need of integrating the analysis of different tasks and processes, acknowledging - rather than simply reducing - their complexity and non-linearity. As a consequence, the "reductive tendency" of designers of complex socio-technical systems should be avoided, making room for a complexity management perspective (Pavard & Dugdale, 2006). On this path, this paper adopts the Functional Resonance Analysis Method (FRAM) to analyse a process in the railway domain, extending the traditional FRAM by a semi-quantitative and multi-layer framework.

2 AN INNOVATIVE COMBINED APPROACH FOR FRAM

FRAM aims at defining complex systems analyzing their functional aspects rather than their physical structure. It allows showing actual interactions, in terms of how a system actually performs in everyday work, adapting their functioning to deal with the variability of current operating conditions.

2.1. The Traditional FRAM

FRAM relies on four principles: equivalence of failures and successes, approximate adjustments, emergence, and functional resonance. The traditional building process of a FRAM model consists of four steps, i.e. identification and description of system's functions, identification of performance variability, aggregation of variability, management of variability. The proposed framework does not affect FRAM principles, but modifies its building steps, as detailed in §2.2 and §2.3. In the proposed framework, the basic element of a FRAM model, i.e. a function described according to six aspects (Input, Output, Precondition, Resource, Control and Time), remains the core of the analysis. For a complete and detailed description of FRAM principles and building steps, refer to Hollnagel's handbook on FRAM (Hollnagel, 2012).

2.2. A Multi-Layer Framework for FRAM

The idea of a multi-layer FRAM arises from the consciousness that in a complex system, a single representation does not allow describing and coping with different scenarios, each one characterized by different requisites. As argued by Rasmussen in 1970, it is beneficial to explore a complex work domain by his two-dimensional representation: the abstraction/decomposition framework. The decomposition (on x-axis) represents the physical aggregation levels of the system (from whole system to smallest components). The abstraction (y-axis) represents the degree to which the physical implementation of functions is maintained in the representation (Rasmussen, 1985). A representation in these two dimensions allowed describing and transferring the analysis of the work domain to different resolution levels.

On this path, a recently introduced framework in the field of risk and safety management is adopted: the Abstraction/Agency framework, combined with FRAM (Patriarca, Bergström, & Di Gravio, 2017). Even if its abstraction dimension follows the traditional Rasmussen definition, the agency dimension (x-axis) aims at exploring different abstraction levels following the perspective of different system's agents. The number of abstraction levels as well as the number of agents are not absolute, depending on the purpose of the analysis, and on the characteristics of the system itself. Once defined the agents to consider for the purpose of the analysis, the framework aims at managing the complexity of the resolution, allowing limited analyses only to significant abstraction levels. Furthermore, it allows filtering the functions (i.e. the hexagons) of a FRAM model, generating multiple representations of the same model at different abstraction levels, and/or for different agents. The framework helps giving sense to the spatial representation of the system, allowing a standard representation to increase the comprehensibility of the model. It is interesting to observe how this multi-abstraction level does not compromise the *method-sine-model* assumption of FRAM. It rather suggests a complexity management perspective, maintaining the scale invariance of FRAM, yet argued by Hollnagel himself (Hollnagel, 2012). Figure 1 sketches a theoretical Abstraction/Agency framework, representing the same generic FRAM function (function k-th) performed by a generic agent (agent g-th). Note that the n_g number of abstraction levels can be different for each agent, depending on the purpose of the analysis.

In a methodological perspective, for using the Abstraction/Agency framework, it is necessary to intervene in the first building step "identification and description of system's functions". Once the analyst has defined the functions at the n_g-th abstraction level following the traditional approach, he has to ascribe them to the g-th agent who actually performs it, who can be an individual, a group of them, an artefact, etc. Then, for each function at the n_g-th abstraction level, the analyst has to assign name and descriptions of the $(n_g - 1)$ functions at the upper abstraction levels, defining the respective function names. Note that those functions at the remaining $(n_g - 1)$ abstraction levels will be inherently defined in terms of the six aspects by a functional envelope of the functions at the n_g-th abstraction level. This approach is in line with the purpose of the Abstraction/Agency framework, which does not aim at developing different models of the same work domain (adding more hypothesis on its functioning), but creating different resolutions of the same work domain at different abstraction levels.

2.3. A Semi-Quantitative Framework for FRAM

Research on FRAM recently shows an increasing interest in variability and uncertainty modelling, combining the traditional method with other relevant approaches. For example, showing the benefits of checking paths of variability by the aid of the model checker SPIN (even if limited to simple systems) (Yang, Tian, & Zhao, 2017); using the Analytic Hierarchy Process (AHP) to increase objective assessment of functions' variability (Rosa, Haddad, & de Carvalho, 2015). Furthermore, Monte Carlo simulation has been used to explore variability, showing the benefits of its application in combination with FRAM in the air traffic management system (Patriarca, Di Gravio, & Costantino, 2017), and process plant (Patriarca, Di Gravio, Costantino, & Tronci, 2017). In a methodological perspective, Monte Carlo simulation affects the building steps "identification of performance variability" and "aggregation of variability", with inherent consequences even in "management of variability".

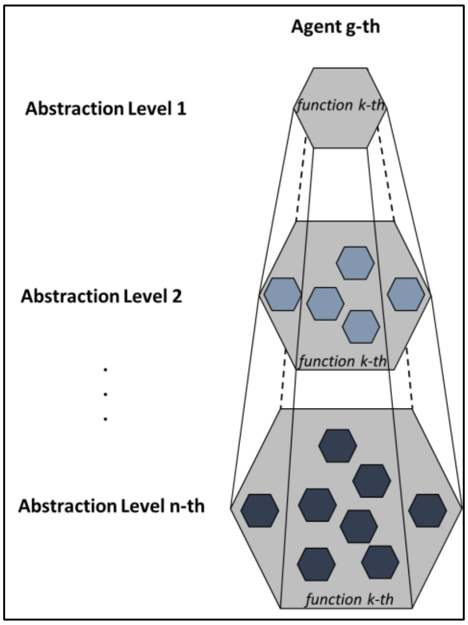


Figure 1. Theoretical representation of the Abstraction/Agency framework. The hypotheses of fractality and scale invariance allows a multi-layer representation of the same k-th function, performed by the g-th agent.

In the process of "identification of performance variability", the first phase consists of defining the phenotypes of variability (i.e. manifestations of variability). Even if it would be possible to adopt a large set of phenotypes, a simple solution consists of considering two of them: timing and precision (Hollnagel, 2012). In terms of timing an output occurs (e.g.) too early, on time, too late or even not at all. In terms of precision, the same output can be precise, acceptable, imprecise or wrong. For the semi-quantitative framework used in this research, it is necessary to assign a numeric score to functions' variability, based on the criticality of its variability state. Since functions' behaviour is not deterministic and static, it is necessary to define a probability distribution of potential states of variability, which corresponds to a distribution of scores. Under the assumption of independent states of variability for the two phenotypes, the variability of a function's output OV_j can be expressed as the product of two distributions: V_j^T, representing the score distribution in terms of timing, and V_j^P representing the score distribution in terms of precision, both for the j-th output. Monte Carlo simulation allows calculating OV_j, which is the distribution of variability for the j-th output (Output Variability) in terms of criticality:

$$OV_j = V_j^T \cdot V_j^P \quad (1)$$

For the "aggregation of variability" step, it is necessary to understand how the output's variability affects its upstream/downstream couplings. Following the connections described in the FRAM model, an output may relate to different functions, generating different effects depending on the output's variability (i.e. its score) and the specific aspect it is linked to (i.e. the upstream/downstream connection), as stated by the principle of functional resonance (Hollnagel, 2012). The upstream/downstream connection might generate an amplification or a damping effect, or can be negligible. On this path, the two indexes a_{ij}^T and a_{ij}^P represent the amplifying factor for the connection between the j-th upstream output and the i-th downstream function, respectively in terms of timing and precision. Their values can be exactly 1 in case of no functional resonant effect, greater than 1 in case of an amplifying effect, and minor than 1 for a damping effect. A probability distribution function CV_{ij} represents the Coupling Variability for the j-th upstream output and the i-th downstream function:

$$CV_{ij} = OV_j \cdot a_{ij}^T \cdot a_{ij}^P \quad (2)$$

Lastly, for the "management of variability" step, once a CV_{ij} is ascribed to each link in the model, it is possible to filter the couplings based on their values over a threshold CV^*. Once assigned a confidence level P^*, a coupling will be considered critical if CV_{ij}^*, i.e. the cumulative distribution of CV_{ij} over CV^*, is greater than $(1 - P^*)$. This classification helps ranking the couplings based on the cumulative distribution value over the threshold, in order to define mitigating actions for managing the negative effects of functional resonance. The scores, as well as the effects of performance variability and the definition of the threshold have to be determined based on available data and on the judgments of Subject Matter Experts (SMEs), who play a crucial role for the application of the described semi-quantitative framework.

3 ILLUSTRATIVE EXAMPLE

This section provides some indications about the application of the framework for a railway incident happened in November 2005 between Esher and Hampton Court Junction in UK. The event caused no injuries to people and no direct damage to the infrastructure, but it caused serious negative effects on the traffic of the track. The immediate cause described in the RAIB incident report was low adhesion on the up fast line, as a direct consequence of the presence of contaminants on the rail and no previous rail treatment (Rail Accident Investigation Branch, 2008). This paper summarizes the outcomes arising from the application of the FRAM semi-quantitative framework combined with the Abstraction/Agency framework. The work presented in this paper starts from a recently published research (Patriarca, Bergström, et al., 2017) that developed the Abstraction/Agency framework for the same incident, as an illustrative case study to explain the feature of the framework itself, without discussing the actual work domain.
The FRAM analysis started with the official RAIB report, used as a starting point to analyse procedures, standards, and other reports with similar low adhesion issues in UK. Note that the Esher incident was one of several adhesion-related events happened during the autumn of 2005 in UK. The focus group was made up of 5 people: two researchers with experience in FRAM modelling and an engineering background, one researcher with a background in railway engineering, two SMEs (one train driver and one railway signaller, both with 10+ years of work experience with similar trains). The analysis included in this paper does not aim to be a complete and exhaustive incident analysis; it rather aims at illustrating the potential benefits of a combined multi-layer semi-quantitative framework for FRAM. Figure 2 details the Abstraction/Agency framework, which includes 6 Agents, and 4 abstraction levels, whose meaning is discussed in (Patriarca et al., 2017a, p. 38).

Agency / Abstraction	AGENT 1 Industrial Committee for Standards	AGENT 2 Weather Forecast Company	AGENT 3 Infrastructure Company	AGENT 4 Signaller	AGENT 5 Train Company	AGENT 6 Driver
FUNCTIONAL PURPOSE (FP)	1 FP	1 FP	1 FP	1 FP	1 FP	1 FP
GENERALIZED FUNCTION (GF)	1 GF	1 GF	3 GF	5 GF	2 GF	8 GF
PHYSICAL FUNCTION (PF)	Not analysed	2 GF	17 PF	18 PF	Not analysed	29 PF
PHYSICAL AND TECHNOLO-GICAL FORM (PTF)	Not analysed	Not analysed	Not analysed	Not analysed	Not analysed	13 PTF

Figure 2. Conceptual Abstraction/Agency framework developed for the analysis. The analysis focused mainly on the actions of the Driver, as proved by the interest in using the maximum levels of abstractions for its modelling, i.e. PTF (Patriarca, Bergström, et al., 2017).

The framework helped organizing the FRAM functions by a structured representation to manage the complexity of representation with sensible benefits, if compared with traditional modelling (as observed by the two researchers in the focus group with experience in FRAM). As an outcome of the framework it has been possible to develop several intra-agent inter-level, intra-agent intra-level analyses, as theoretically described in (Patriarca, Bergström, et al., 2017). As a further development, the Monte Carlo framework, allowed performing systematically several of these analyses, with the purpose of extracting the more critical couplings, based on the effects of their variability. As a first step, as discussed in § 2.3, two phenotypes of variability have been identified, i.e. timing and precision, assigning then a score for each state, as detailed in Table 1. Then, each output of the model at the $\boldsymbol{n_g}$-th abstraction level has been described in terms of its variability, relying on the analysis of other reports of similar train and infrastructure conditions and moreover on the experience of the SMEs involved in the focus group, who described their activities in everyday work. Since FRAM relies on normal work, work-as-done, the experience referred by the SMEs acquired a crucial role for defining the model and its inherent variability. For each output, by operational data (where available, e.g. meteo conditions) and the analysis of normal work in semi-structured interviews, $\boldsymbol{V_j^T}, \boldsymbol{V_j^P}, \boldsymbol{a_j^T}, \boldsymbol{a_j^P}$ have been assinged, following Table 1. At this step, the Abstraction/Agency framework has been explored by Monte Carlo simulation in order to understand and get indications on how to manage the variability of the process. A coupling has been considered critical if the $\boldsymbol{CV_{ij}^*}$ cumulative distribution over a threshold exceeded $\boldsymbol{CV^*} = \mathbf{8}$, with a confidence level $\boldsymbol{P^*} = \mathbf{0.95}$. The threshold $(\boldsymbol{CV^*} = \mathbf{8})$ can be interpreted to isolate those outputs whose variability has limited consequences on the process $(\boldsymbol{V_j^T} = \boldsymbol{V_j^P} = \mathbf{2})$ but with a least an amplifying effect $\boldsymbol{a_j^T}(\boldsymbol{or}\ \boldsymbol{a_j^P}) = \mathbf{2}$.

The Monte Carlo simulation has been applied for an inter-agent inter-level analysis for Agent 6, i.e. Driver at the abstraction level of Physical Functions (PFs). The variability on the retardation rate observation plays a crucial role with a very high value of the cumulative probaiblity voer the threshold ($\boldsymbol{CV^*_{ij}} = \mathbf{0.22}$), leading to activate the braking management functions (see Figure 3A). Furthermore, an inter-agent intra-level analysis has been applied to assess the interactions between the Driver's PFs and the Generalized Functions (GFs) performed by the other agents. In this case, the in-loco low-adhesion warning signals appear to have a crucial role ($\boldsymbol{CV^*_{ij}} = \mathbf{0.45}$) for Driver's awareness (see Figure 3B) and then preparedness to manage successfully abnormal adhesion conditions and braking actions (this coupling represents an example of an intra-level criticality).

Table 1. *Semi-quantitative parameters used in the Monte Carlo framework.* $\boldsymbol{V^T_j}, \boldsymbol{V^P_j}, \boldsymbol{a^T_j}, \boldsymbol{a^P_j}$ *are probability distribution functions defined by the corresponding values fo the variability state assigned in the analysis.*

$\boldsymbol{V^T_j}, \boldsymbol{V^P_j}$ **score**	**Criticality effect**	$\boldsymbol{a^T_j}, \boldsymbol{a^P_j}$ **score**	**Criticality effect**
1	The output variability has *no critical implications* on the process	**0.5**	The output has a *damping effect* on the variability of upstream/downstream coupling)
2	The output variability has *limited consequences* on the process	**1**	The output has *no effect* on the variability of upstream/downstream coupling)
3	The output variability has *relevant consequences* on the process	**2**	The output has an *amplifying effect* on the variability of upstream/downstream coupling)
4	The output variability has *dangerous consequences* on the process		

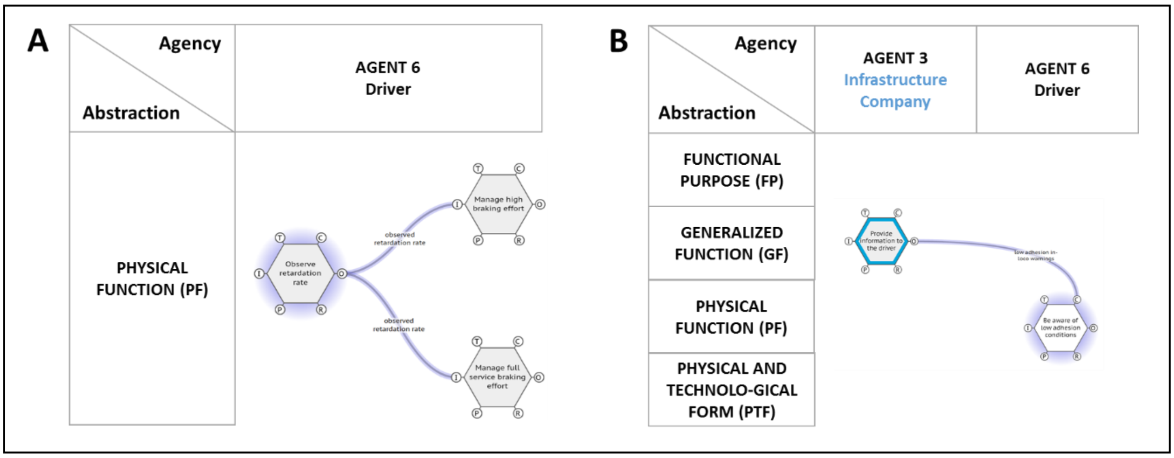


Figure 3. Examples of critical couplings emerged from the Monte Carlo simulation applied to the Abstraction/Agency framework: A) coupling emerged from a semi-quantitative inter-agent inter-level analysis (at PF level); B) coupling emerged from an inter-agent intra-level analysis (between PF and GF levels).

4 CONCLUSION

This paper shows how a traditional FRAM analysis can be combined with Monte Carlo simulation and with the Abstraction/Agency framework. The combined approach appears particularly relevant for systematic inter-agent inter-level, or inter-agent intra-level analysis, helping the analysts managing complexity by looking at the same model using different resolutions. The semi-quantitative approach allows filtering the complexity of representation, ranking the couplings' criticality. This results might be potentially helpful to develop more detailed monitoring indicators (sensors, specific questionnaires, reporting procedures, etc.) which can be used to gather real data and define proper mitigating actions (Albery, Borys, & Tepe, 2016), other than feeding the simulation model to refine the analysis. This purpose can be achieved starting from a detailed analysis of the more critical couplings, i.e. the ones with higher CV^*_{ij} (e.g., referring to Figure 3, discussing how to improve the in-loco warning signals, or performing an observational study to understand how in everyday work the observation of retardation rate is actually delayed).

The Abstraction/Agency framework allows developing a more comprehensible FRAM model, with potential implications for risk assessment and accident analysis, and even for organizational knowledge management. The Monte Carlo framework allows highlighting which sources of variability have to be damped, or enhanced, gaining a deeper knowledge of the process under analysis, helping decision-makers defining short-term and long-term actions to enhance safety and performance levels. A Monte Carlo multi-layer approach helps understanding system failure according to complexity theory, which prescribes "going up and out" to explore how functions are related at different abstraction levels with different agents (Dekker, 2011). The approaches described in this paper for illustrative purpose (with no pretension to be an exhaustive incident analysis) can be adapted in different socio-technical systems, for the analysis of both performance and safety parameters.

REFERENCES

Albery, S., Borys, D., & Tepe, S. (2016). Advantages for risk assessment: Evaluating learnings from question sets inspired by the FRAM and the risk matrix in a manufacturing environment. *Safety Science*, *89*, 180–189.

Dekker, S. (2011). *Patient Safety - a human factor approach*. Boca Raton, FL: CRC Press - Taylor & Francis Group.

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*. Ashgate.

Hollnagel, E., Leonhardt, J., Licu, T., & Shorrock, S. (2013). From Safety-I to Safety-II: a white paper. *Brussels: European Organisation for the Safety of Air Navigation (EUROCONTROL)*.

Pasmore, W., Francis, C., & Haldeman, J. (1982). Sociotechnical systems: A North American reflection on empirical studies of the seventies. *Human Relations*, *35*(12), 1179–1204.

Patriarca, R., Bergström, J., & Di Gravio, G. (2017). Defining the Functional Resonance Analysis space : combining Abstraction Hierarchy and FRAM. *Reliability Engineering & System Safety*, *165*(February), 34–46.

Patriarca, R., Di Gravio, G., & Costantino, F. (2017). A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems. *Safety Science*, *91*, 49–60.

Patriarca, R., Di Gravio, G., Costantino, F., & Tronci, M. (2017). The Functional Resonance Analysis Method for a systemic risk based environmental auditing in a sinter plant : A semi-quantitative approach. *Environmental Impact Assessment Review*, *63*, 72–86.

Pavard, B., & Dugdale, J. (2006). The contribution of complexity theory to the study of socio-technical cooperative systems. In A. A. Mina & A. M. Y. Bar-Yam (Eds.), *Unifying Theories in Complex Systems (Volume IIIB)* (pp. 39–48). Berlin, Germany: Springer.

Rail Accident Investigation Branch. (2008). *Rail Accident Report - Autumn Adhesion Investigation Part 1: Signals WK338 and WK336 Passed at Danger at Esher 25 November 2005* (Vol. 25 (Part 1).

Rasmussen, J. (1985). The role of hierarchical knowledge representation in decision making and system management. *IEEE Transactions on Systems, Man, and Cybernetics*, *SMC-15*(2), 234–243.

Rosa, L. V., Haddad, A.N., & De Carvalho, P.V.R. (2015). Assessing risk in sustainable construction using the Functional Resonance Analysis Method (FRAM). *Cognition, Technology and Work*, *17*(4), 559–573.

Stamatelatos, M. (2002). Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. *Office*, (December), 1–323.

Vaughan, D. (1996). *The Challenger Launch Decision*. Chicago and London: The University of Chicago Press.

Yang, Q., Tian, J., & Zhao, T. (2017). Safety is an emergent property: Illustrating functional resonance in Air Traffic Management with formal verification. *Safety Science*, *93*.

CITY RESILIENCE: ANALYSIS OF STRATEGIES WORLD-WIDE

Amy Rankin[1], René Lindner[2], Maider Sainz[3] Simon Rosenqvist[4], Magnus Bång[5] and Henrik Eriksson[6]
[1,3,4] Department of Computer and Information Science, Linköping University, Sweden
[1]amy.rankin@liu.se +4613282757
[4]simro275@student.liu.se, [5]magnus.bang@liu.se, henrik.eriksson@liu.se
[2] DIN, Berlin, Germany
rene.lindner@din.de
[3]Tecnun University de Navarra, Donostia-San Sebastian, Spain
msainz@tecnun.es

Abstract

In recent years, resilience has become an important goal for cities, particularly in the face of political uncertainty, climate change and increasing urbanisation. Resilience theory has yielded informative lessons and brought new perspective when preparing for, and responding to vulnerabilities cities face today, such as natural hazards and social inequalities. However, critical questions on how to operationalize resilience through political decision making and community engagement are still unanswered, and supporting methods and concrete action plans are needed. In this paper, we offer an overview of the result from three studies conducted as part of an ongoing H2020 research project, Smart Mature Resilience. The three studies inlucde a literature review of definitions and approaches in city resilience, analysis of city resilience strategies and requirements for standardization. Key findings from the studies are presented and implications of their findings for the development of resiliience management guidelines are discussed.

1 INTRODUCTION

Increasing resilience to crises and disasters is a topic of highest political concern worldwide. The need for cities to prepare for, prevent and manage the effects of natural hazards and man-made threats such as floods, storms, earthquakes, tsunamis, accidents and terrorism is becoming increasingly imminent. This need is reflected in recent initiatives. In 2015, the UN General Assembly endorsed the Sendai Framework for Disaster Risk Reduction 2015-2030 (UNISDR, 2015), aiming to achieve reduction of disaster risk in economy, social issues, cultural assets and environmental resources over the next 15 years. In addition, Resolution 339 was adopted by the Council of Europe and the aim is to support the UN campaign "UNISDR Making Cities Resilient" to implement local adaptation processes such as sharing best practices and developing partnerships between countries. Similarly, the OECD provides a comprehensive report supporting the Sendai Framework and the New Urban Agenda of the UN though its analysis of approaches, policies and concrete city actions worldwide (OECD, 2016). Another world-wide network in focus in this paper is the 100 Resilient Cities[3] (100RC) initiative, established by the Rockefeller Foundation, aiming to support and improve resilience at the community-level worldwide (Arup, 2014).

The growing political interest in resilience approaches to tackle future challenges is an important first step. However, current frameworks have been criticized for being of limited relevance to local realities and lack an understanding of the complex risk landscape that shape todays cities (Oxley, 2015). Recent literature reviews on city resilience show concurring findings, including a great variety in attributes and indicators used, reflecting the lack of consensus and unification of central themes (Meerow, Newell, & Stults, 2016; Rankin et al., 2016). An important challenge is going from theory to practice, that is, from theoretical models of resilience to methods and concrete action plans.

Smart Mature Resilience[4] (SMR), a current H2020 European project, aims to address some of these issues by developing, testing and validating European Resilience Management Guidelines (ERMG) for city resilience operationalised through five support tools: 1) a Resilience Maturity Model defining the trajectory of an entity (system, community or society) through measurable resilience levels; 2) a Systemicity Risk Questionnaire that, beyond assessing the entity's risks, also includes analysis of interdependencies between risks and potential cascading effects; 3) a portfolio of Resilience Building Policies that support the entity's progression towards higher maturity levels; 4) a System Dynamics Model (computer simulation model) that embodies the Resilience Maturity Model, allowing to diagnose, monitor and explore the entity's resilience trajectory as determined by

[3] http://www.100resilientcities.org/

[4] http://www.smr-project.eu/home/

resilience building policies, and 5) a Resilience Engagement and Communication Tool to integrate the wider public in community resilience, including public-private cooperation. Further, a European standard will be developed based on the ERMG, supporting sharing of data and facilitating comparisons between cities in Europe. Several studies have been conducted to gather needs and requirements for the ERMG. This paper presents key findings from three of these studies; (1) literature review of academic articles and world-wide reports on city resilience, (2) city resilience strategy analysis of 18 cities and (3) standardization requirements for development of a standard. The final section of the paper identifies a set of implications from the results for guidline development.

2 LITERATURE REVIEW: KEY FINDINGS

To gain insights into how resilience in a city context is defined, discussed and applied, a review of 119 peer-reviewed journal articles and 23 reports on world-wide city resilience initiatives was carried out (Rankin et al., 2016). The analysis of the research articles focused on three overarching areas; resilience definitions and problem areas, related concepts and applications of resilience. The reviewed reports came from organisational bodies and cities worldwide, and focus areas for our analysis were resilience implementation, evaluation, metrics, best practices, and policies. Below, we present key areas from the reviewed literature identified as requiring particular attention. For the full description of the method and results see Rankin et al. (2016).

2.1 Conceptual Tensions

The literature demonstrates a large variety in definition and approaches, reflecting a lack of consensus and unification on the notion of city (and urban) resilience. The lack of consensus also reflects the vast number of areas and goals that are important to resilience and city management. Several "sub-fields" of relevance to city resilience were identified, such as, community resilience, social resilience, crisis/disaster resilience, infrastructure/engineering resilience and economic resilience. Definitions between and within the different fields vary, including some fundamental differences in perspectives and assumptions made. For example, literature on disaster resilience tends to focus on cities ability to "*bounce back*", that is, to recover from an event and "get back" to its previous state (Manyena, 2006). In infrastructure and engineering resilience, definitions focus to a higher extent on abilities to "*absorb*" disturbances, and in community and socio-ecological resilience highlights *adaptive abilities* to on-going circumstances (Folke, 2006).

The different theoretical perspectives have distinctive implications on how research and applications of resilience should be managed (see Woods, 2015). It may be argued that different aspects of the resilience concept are suited for different areas of city resilience; as goals vary between different parts of the urban system. For example, with regards to critical infrastructure, the ability of a network to cope with, or "absorb" short-term disturbances through robustness and redundancy may be a key feature, whereas a key property of a resilient community is its ability to adapt to both short- and long-term changes. Moreover, the fundamentally different use of terminology in this area can be an obstacle making collaborative efforts between researchers, politicians, private companies and citizens difficult.

2.2 Safety I and Safety II - Dependencies and Cascading Effects

Frameworks for city resilience, such as the Sendai framework (UNISDR, 2015) and the 100RC Resilience Framework (Arup, 2014), still have a focus on risk reduction, rather than on a holistic approach including both risk management (Safety-I) and general capacity and flexibility (Safety-II). Main topics of the analysed frameworks include: understanding and education on disaster risk, strengthening disaster risk governance, investing in risk reduction and enhancing responsiveness. The focus on risk and a faulty conceptualization of resilience solely as risk reduction management may seriously reduce the understanding of the complexity of the issue since many cities already have a risk management approach in progress, and hence "resilience". However, to help deal with the complex issues of increasingly interdependent systems, resilience has to go beyond traditional approaches of relying on predictions and risk reduction, and focus attention on *general capacity* to tackle a broad range of risks helping cities prepare for combined impacts and unintended consequences. As discussed by the 100 Resilient Cities Network (100RC, 2016) risks may take different forms, as (sudden) acute shocks, but also gradually evolving chronic stresses. Resilience is about being pro-active, with the aim to prepare systems to cope with variation through adaptation and flexibility, and to stay alert to system variations and the changing shape of risk (Hollnagel, 2011).

However, identifying feasible ways to model and analyse the dependencies and cascading effects of disturbances is a big challenge. For example, changes and disturbances in a cities infrastructure almost never have a single effect on the city's resilience but can have far-reaching effects in many different realms of society. If the electric power grid, water supply and communications (transport and ICT) infrastructure is not secured during a crisis the batteries in cellular towers will be depleted and all communication will be affected. However, the infrastructure sits within complex national and global frameworks with inherent co-dependencies and weak points. The dependencies, numerous stakeholders (subcontractors) and legal frameworks render the management of infrastructures on the local level difficult. Reverberating effects and events and actions should, however, not only be seen in the light of increased risks and vicious circles; effect may also be positive. City initiatives show that individual projects such as a park can give the community members not only a green place to spend their afternoon, it can also be a meeting place for different groups to support social cohesion. Additionally, its permeable soil can increase resilience against flooding and decrease effects of heat waves. The trees absorb green-house gases and the park is a place of education where the community can learn about ecological principles.

Attempts to model dependencies, cascading effects and reverberations within a city is, besides individual case-studies, only done on a very high level (Hagen, Tzanetakis, & Watson, 2015). The challenges in developing generalisable frameworks and models for complex entities like cities are manifold, including the identification of boundaries and scope, interconnected and influencing factors, combined effects of risks, vicious feedback loops and contextual dependence (Rankin et al., 2016).

2.3 Going from Theory to Practice

From our literature studies it is clear that existing resilience frameworks are abstract and high-level, which means that there is a lot of work required to contextualise and implement existing models and methods on the city level. A benefit of using high-level concepts are that it offers a way to include many areas, and an abstract way to consider the multiple processes and stakeholders involved, and their interactions. The downside of more general models is that they must be translated to a specific context, which can be cumbersome and challenging for practitioners. Challenges include untangling and contextually defining multiple dimensions and parameters of complex cities, as well as prioritizing action and definition indicators.

Additionally, as mentioned earlier, the current literature review underlines the lack of consensus of the resilience concept and how it should be included in the frameworks. The large variety of framework attributes/indicators makes comparisons of the frameworks challenging, which makes it difficult for city representatives to apply resilience in everyday work.

3 CITY RESILIENCE STRATEGIES ANALYSIS: KEY FINDINGS

The resilience strategies prepared by 18 cities being part of the Rockefeller Foundation network of 100 Resilient Cites[5] was analysed. The data consisted of official documents and webpages. The study focussed on identification of the subjective challenges the city faced, goals of the resilience work, and plans of action to approach identified goals. All five continents are represented in the analysis, including five cities in North America, four in South America, two in Asia, three in Europe and two in Australia (for the analysis see Rankin et al. (2016)). The analysis was performed coding the data with a subsequent thematic analysis (Braun & Clarke, 2006), with the goal to capture city challenges and planned actions. Three top-down categories were used in the analysis: (1) vulnerabilities, (2) approaches and, (3) affected groups. Furthermore, a bottom-up approach was applied to the data, allowing sub-categories to take form, nuancing the data.

Following the analysis, a set of interviews were carried out with six city representatives from three different European cities involved in the process of developing and implementing the city strategies. Two of the cities were in the process of finalising their strategy and one city had completed the strategy and was in the early stages of implementation. The interview was centred on the process of developing and carrying out the strategy.

3.1 City resilience strategies: Vulnerabilities, solutions and affected groups

The vulnerabilities can broadly be classified under the categories of social issues, climate change and critical infrastructure. Vulnerabilities associated with social dynamic vulnerabilities were first and foremost concerned with different forms of social exclusion (e.g., unemployment, immigration, elderly) and the lack of access to societal services such as health care. Vulnerabilities regarding climate change were either concerned with the general topic of increasing levels of greenhouse gases, or more specific threats such as flooding, draught, storms,

[5] http://www.100resilientcities.org/strategies#/-_/. At the time of analysis only 18 cities had finalised their strategy.

or earthquakes. Under the theme of critical infrastructure, common vulnerabilities were water access and waste disposal. The reports also suggested that the cities are concerned with how to maintain communication and transportation services in the face of a disaster. With regards to social issues, cities aim to approach internal management silos as well as improving communication with citizens, business and other stakeholders. A common approach to tackle challenges included creating community plans and expanding present programs/plans. A widely-applied solution was to modify the evaluation processes of already existing projects to also include aspects of resilience, with the aim to make it an integral part of policy-making and everyday operations. Involved stakeholders varied between the three different categories. Solutions related to social issues, on the other hand, commonly involved the ambition for collaboration within the community and its initiatives, as well as creating new business partnerships. With regards to climate change, responsibility were often directed toward the local government and solutions in the form of policies, such as enforcing city departments to lower their energy usage. In the critical infrastructure category, the local government was commonly described as a single actor, making plans for future projects and related knowledge-gaining activities.

To conclude, the results indicate that the resilience strategies and concrete actions of the 100RC cities are mainly focused on measures to improve community cohesion, information gathering (monitoring), and resilience-thinking based on graceful management of “disasters” (e.g. being in control of a flood). Furthermore, the solutions proposed were in many cases multifunctional and multipurpose, suggesting that cities put effort into identifying dependencies between identified vulnerabilities and potential effects the solutions may have in the long and short term.

3.2 City Resilience Strategies: Results from Interviews

The interviews with city representatives focused on the process of developing a strategy and related problems. Main challenges mentioned illustrate well the issues discussed in the literature with regards to operationalising a broad concept to a complex system. Two main issues surfaced in all interviews:

- Politics and collaboration - this issue concerns who “owns” a problem and how to coordinate the many involved stakeholder, both public and private, and getting necessary expertise and involvement.

Resilience is not a solo project, but rather something closely tied to multiple activities in the city, such as city planning, crisis preparedness, health care and critical infrastructure. The interconnectedness forms a challenge of getting necessary stakeholders and expertise involved to propose a feasible resilience strategy. In many cases the involvement is voluntary, and thus the initiatives must be sufficiently “inviting” to all partners. Furthermore, in larger cities it is not possible to have a single and central administration as it is divided into districts. Who “owns” key areas, such as waste management, public transportation and policing may vary between the central government and the individual district. In Rome, for example, this difficulty was solved by dividing the strategy mapping into two different sectors, one being experts in key fields, and the other being the general population.

- Politics and prioritization - cites have different preconditions and starting points. Identifying and prioritizing an action plan for the local context is challenging. Further, trade-off priorities, politics and funding play an important role.

The second main issue found in the interviews is knowing how to prioritise actions. When it comes to resilience, a lot of work in areas such as social issues and climate change is already seen as being performed, and it is not always clear to city representatives how the concept of resilience will change or strengthen the current efforts. Adding to this issue is the difficulty of city politics, getting projects funded, and the need to be able to motivate and prove idea. One city representative gave the example of how a change in government following an election led to a shutdown of on-going projects and major difficulties in receiving new funding.

4 STANDARDIZATION REQUIREMENTS: KEY FINDINGS

It has been argued in this paper that a main challenge in developing tools for city resilience is the need for highly contextualised and local solutions. At the same time, general approaches are important to support world-wide initiatives, foster sharing of data and facilitating comparisons. In this regard, standardization is a tool that supports the dissemination and exploitation of results from research and innovation. Within the SMR project, part of the Eurpoean City Resilience Guidline will be transformed into a standard. This will be done in three stages: (1) identify related existing standards, (2) gather user requirements and (3) development the standard

document through a CEN[6] Workshop. The CEN workshop includes a series of workshops with field experts, and results on a standards document, also called the CEN Workshop Agreement (CWA) [7].
The comprehensive review of existing standards relating to the topic of city resilience resulted in a list of 270 identified existing standards (Linder & Kempen, 2016), demostrating again the broadness of the resilience concept. This collection includes related areas such as sustainable development and societal security. Within these areas existing standards offer, for example, guides to establishing strategies for smart cities and communities, indicators for resilient cities and guidance for managing security in healthcare facilities.

User requirements from city representatives have been gathered through a survey, and followed by a joint workshop of all survey participants and external city representatives. Questions in the survey related to the current use of standards, how standards are shared among city experts and the need for new standards. Results from the survey showed that current use of standards mainly refer to management standards relating to general topics such as quality (EN ISO 9001), environment (EN ISO 14001) and energy (EN ISO 50001). Standards addressing more specific topics related to resilience are generally unknown by the city representatives, e.g., scenario planning - Guidelines for decision making processes dealing with climate change (DIN SPEC 35811). The survey participants reported a need for a new standard supporting three main areas; (1) development of responsive structures within the city (2) cross-sectorial collaboration between city stakeholders and, (3) processes to include citizens in the resilience process. Furthermore, the results show that the city representatives require resilience approaches that can be incorporated into already existing projects and initiatives such as sustainability and smart city.

In the next phase the scope of the standard will be identified, based on an analysis of important existing standards and city requirement. The process of the CWA will support the integration of these two parts. The open structure of such a CWA allows transparency towards all involved stakeholders and interested parties and it ensures a broad consensus of a potential standard's contents. Cities representatives therefore have the possibility to be part of this process; which enhances the future adaption by a wide range of cities. Further, the standard will be available to all European cities, with the goal to support and facilitate resilience development in cities, as well as information sharing between cities. In this regard, the developed city resilience standard will bring together existing standards and the findings from the project research, inlcuding findings from the literature and the user requirements gathered from city representatives.

5 DISCUSSION: IMPLICATIONS FOR DEVELOPMENT OF RESILIENCE MANAGEMENT GUIDELINES

The findings from the studies outlined in this paper support continued work in the development of guidelines, practical tools and standards for city resilience. The main implications for further research are outlined below.

- **Joint understanding of the resilience concept and objectives**

The literature review shows that the application of resilience in a city context is fragmented. Different definitions, goals and approaches are used, creating conceptual tensions and challenges in unifying resilience research and initiatives. Implications of different resilience viewpoints are found in the assumptions, objectives, measurements and improvements made by researchers and practitioners. It is thus of utmost importance to carefully consider, discuss and agree on definitions, objectives, viewpoints and strategies with all involved stakeholders, to ensure joint understand of the conducted work. This may be done through, for example, the process of standardization.

- **Identification of risk dependencies, cascading effects and reverberations**

There is a consensus in the literature that research and initiatives in urban resilience has overlooked important couplings between different dimensions of community management, including both social and physical aspects. Indeed, the risks which cities face are usually the consequence of complex interactions between many factors which can often reinforce one another. These interactions can lead to non-obvious, and counter-intuitive, unintended consequences that may be difficult for cities to anticipate. In other words, for practitioners in the public sector, it is limiting to view risks as being independent, instead it is essential to understand risks as forming complex networks. Therefore, suitable tools are needed that can support city staff to identify and explore how risks interact with each other and potentially can affect the city planning. Models and tools should thus compliment current risk assessment approaches and offer practical tools which could be used by cities to

[6] https://www.cen.eu/work/products/CWA/Pages/default.aspx; CEN is the European Committee for Standardization.

[7] https://www.cen.eu/work/products/CWA/Pages/default.aspx; CEN is the European Committee for Standardization.

improve their thinking about the dynamics between risks in the short and long terms. Analyses of dependencies further offer guidance for possible positive reverberation that go beyond identified goals. It is expected that by taking a more holistic view on risks, in which the knowledge of various practitioners is pooled together to identify and prevent desirable or undesirable dynamics, cities can become more effective in their preparedness. One way to work on this is to identify and draft possible risk scenarios as a way of preparing for risks, and to consider possible knock-on effects deriving from such scenarios. The analysis of city resilience strategies revealed that some cities have already caught on to this idea, and many current resilience projects address multiple vulnerabilities in different areas of the city.

- **Increased support for adaptive and flexible skills**

Many of the frameworks used for resilience today still have a focus on risk reduction, rather than on a holistic approach including both risk management (Safety-I) and general capacity and flexibility (Safety-II). Models and tools should acknowledge and further support Safety II perspectives. For example, a focus on general capacities, flexibility and multi-stakeholder collaboration across private and public sector will increase resilience and adaptive capacity. Flexible city management processes that foster learning with regards to handling unexpected events is suggested. Policies and metrics should focus on cohesion, communication, flexibility and integration of resilience into the exiting city organisation, budgeting and financing processes. Furthermore, improving the general monitoring capacity is a key to improve resilience. Cities need supporting processes for setting up and using monitoring data at different levels.

- **Balance between generalisation and contextualisation**

Current resilience frameworks are abstract and challenging for city representatives to understand to improve work processes. Hence, there is a need for better guidance to support the development of concrete resilience-oriented work processes that city managers and city employees can apply in everyday work. The study of city resilience strategies showed that the approaches to manage local challenges varied greatly between cities, and were adapted to local possibilities and constraints related to the cities' ecology, geology and history. These findings demonstrate that tools, processes, guidelines, and checklists have to be contextualized and appropriated – hence, they need to allow local adaptions to be made. In the development of tools, such as in the SMR project, require a careful balance between general, high-level resilience concepts, and the specifics of the different settings (i.e., cities). The development of such tools would be an important step in the right direction of going from normative to descriptive models of resilience. Such tools would, ideally, support resilience initiatives on both top-down (high-level policy) and bottom up (local initiatives). However, there is also a need for generalisability to support world-wide efforts, to share results and to ensure common understanding between cities and other relevant parties. To ensure that concepts and processes described in the standards are valuable and adaptable to relevant cities the standardization committee works in close collaboration with the users as part of the development process. Not only are city representatives active participating in the development of the envisaged standard, but an optional public enquiry is further applied to allow a broad range of cities to comment on the standards' content.

REFERNCES

100RC. (2016). What is Urban Resilience? Retrieved May 12, 2017, from http://www.100resilientcities.org/resilience#/-_/

Arup, L. O. P. I. (2014). *City Resilience Framework*. New York, NY.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. http://doi.org/The publisher's URL is: http://dx.doi.org/10.1191/1478088706qp063oa

Folke, C. (2006). Resilience: The emergence of a perspective for social–ecological systems analyses. *Global Environmental Change*, *16*(3), 253–267. http://doi.org/10.1016/j.gloenvcha.2006.04.002

Hagen, K., Tzanetakis, M., & Watson, H. (2015). Cascading effects in crises : categorisation and analysis of triggers. In L. Palen, M. Büscher, M. Comes, & A. L. Hughes (Eds.), *Proceedings of the 12th International ISCRAM Conference*. Kristiansand, Norway.

Hollnagel, E. (2011). Prologue: The Scope of Resilience Engineering. In *Resilience Engineering in Practice: A Guidebook, Vol 2* (pp. xxix–xxxiv). Farnham, UK: Ashgate.

Linder, R., & Kempen, B. (2016). *D6.1 Existing Standards and Standardization Activities Report*. Can be retreived at: http://smr-project.eu/deliverables/.

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters*, *30*(4), 433–50.

Meerow, S., Newell, J. P., & Stults, M. (2016). Defining urban resilience: A review. *Landscape and Urban Planning*, *147*, 38–49. http://doi.org/10.1016/j.landurbplan.2015.11.011

OECD. (2016). *Resilient Cities*. Available at: https://www.oecd.org/gov/regional-policy/resilient-cities-report-preliminary-version.pdf (Accessed 2017-05-10).

Oxley, M. (2015). Review of the Sendai Framework for Disaster Risk Reduction 2015-2030. Middlesex, UK: Global Network of Civil Society Organisations for Disaster Reduction (GNDR).

Rankin, A., Bång, M., Sainz, M., Radianti, J., Lebaka, L., & Hernantes, J. (2016). *D1.1 Survey Report on World-Wide Approaches*. Can be retreived at: http://smr-project.eu/deliverables/.

UNISDR. (2015). *Sendai Framework for Disaster Risk Reduction 2015-2030*. http://doi.org/A/CONF.224/CRP.1

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety*, *141*, 5–9.

A DEBATE ON THE NEW RCA: IS IT A STEP IN THE RIGHT DIRECTION? THE TRADEOFF BETWEEN IMPROVING IDEAS AND IMPROVING SYSTEMS

Michael F. Rayo, PhD[1] and Rollin J. "Terry" Fairbanks, MD, MS[23]
[1] The Ohio State University, Columbus, OH, USA
[1] rayo.3@osu.edu, +16145198809
[1] https://discovery.osu.edu/tda/faculty/members/mike-rayo/
[2] National Center for Human Factors in Healthcare, MedStar Health, Washington, DC, USA
[3] Georgetown University School of Medicine, Washington, DC, USA
rjf48@georgetown.edu, +1-202-244-9811
www.medicalhumanfactors.net/about-us/our-team/rollin-j-terry-fairbanks-md-ms

Abstract

When asked to predict the future success of a new process or method for assessing and making recommendations for system resilience, there is little consensus on what the most advantageous heuristics should be. What attributes of the method should be most closely scrutinized? Which do not matter as much? How does our community ensure that the lexicon of resilience engineering is not misconstrued, misinterpreted, or co-opted by techniques that will ultimately mimic the linear, causal models that we have struggled to dislodge from popular safety management practices? We debate these characteristics in the context of two recent attempts at Root Cause Analysis (RCA) reform in the United States healthcare system. We alternatively praise and criticize these new methods, citing factors such as increased transparency, the risk of shallow analysis, more consideration for frontline practitioners, and lack of mapping to resilience engineering concepts. We hope that this debate serves as a platform for future debates and, ultimately, data-driven consensus on what we attributes we should be prioritizing in future analyses.

1 INTRODUCTION

It has been difficult for the resilience engineering community to know how best to inculcate resilience engineering concepts and precepts into safety management processes. Research findings that are now thirty-five years old are still not broadly reflected in practice. It is widely agreed that current Root Cause Analysis (RCA) processes should be improved to make high-complexity, safety-critical industries safer (Hassall, Sanderson, & Cameron, 2016; Hollnagel, 2014; James, 2013; Leveson, 2004; National Patient Safety Foundation, 2016). However, there is much debate as to exactly what the shortcomings of the RCA are, and what the most advantageous next steps should be. For example, can the structure of the RCA remain in place with minor changes, or does it need to be completely replaced? We discuss two recent initiatives to reform the RCA in the United States healthcare industry, and discuss the merits and potential shortcomings of each. It is our hope that this provides a productive platform to discuss these and future safety management methods and initiatives.

2 PERSPECTIVE 1: THESE SMALL STEPS ARE THE RIGHT STEPS

R.J. (Terry) Fairbanks, MD MS

By and large, hospitals in the United States follow a very consistent process after an adverse event occurs. As noted above, it has been shown by many authors to be not only ineffective but actually damaging to safety culture. In this process, an adverse event occurs and everybody is told not to talk about it, for fear of discoverability during a future deposition. Indeed, plaintiff's attorneys often ask involved providers if they have spoken to anyone about this case. If the answer is yes, they go on to depose the third party. This often causes a fear that leads to lack of transparency, and it is hidden from the patient and their family, hidden from the medical record, and a wall of silence is created, doing further damage to the family and injured patient. In the traditional RCA process, a mandatory meeting is scheduled, often several days or weeks after the event, and usually with leadership present. This is the context in which involved frontline providers come to tell their story. Needless to say, it is unlikely that those empowered to change the system will gain a true understanding of the system in this way. Observers of this process will often tell you that they walk out feeling like members of each department have focused on protecting their own.

However, many organizations are aware of the shortcomings of these methods and have been working to find a better way. In addition to the hospitals that, with the help of external safety scientists, have improved their safety processes, two influential national organizations have created and disseminated new RCA-based safety processes to improve adverse event review. The National Patient Safety Foundation (NPSF) enlisted the help of systems engineers, human factors engineering experts and leaders from Kaiser Permanente and the Veterans Administration safety program to develop the "RCA-squared" (RCA^2) method to improve the quality of adverse event review by emphasizing a systems approach. At the same time, the Agency for Healthcare Research and Quality (AHRQ) funded the creation of a new program called CANDOR. This program shares methods for an immediate response to adverse events, emphasizing transparency and disclosure to patients and their families, care for the caregiver, and a systems based event review process, including individual, non-threatening, one-on-one interviews with those involved (including the patient and family), an early consensus meeting, and a validation meeting that involves leaders who can support change. There is an emphasis on approaching the review with a systems perspective. My perspective is influenced by the fact that I was involved in both of these processes. I served on the committee to advise the development of the in RCA^2, and I was part of a three-person team charged with writing the event review process for CANDOR, which we adapted from an event review process we had recently developed for MedStar Health. For context, MedStar is a large non-profit healthcare delivery system in Washington DC and Baltimore MD (USA) region, with 31,000 employees, $5.4B annual revenue, 300 clinics, and 10 hospitals, including Georgetown University Hospital. During the past seven years, MedStar Health supported the development of an internal group of human factors engineers and cognitive psychologists to support their mission to innovate their approach to safety.

Although neither of these processes are ideal, they are both major steps in the right direction. These areas improvement are perhaps best stated in the goals of CANDOR: encourage event and error reporting by making frontline practitioners feel safe, value firsthand accounts over secondhand accounts, facilitate increased transparency to internal and external stakeholders, and more broadly disseminate the final findings to detect potential hazards earlier.

2.1 Encouraging reporting by making frontline practitioners feel safe

One of the most common contributors to the gap that we typically see between work as imagined and work as performed (Dekker, 2013) is the creation of covert work systems. In covert work systems, frontline practitioners fail to disclose or actively hide certain aspects of work that they believe are essential to the normal function of the system, but if communicated to management would result in admonishment or punishment (Woods, Dekker, Cook, Johannesen, & Sarter, 2010). This includes the tendency of frontline practitioners to underreport errors or events for fear of reprisal. CANDOR addresses this with their care for the caregiver program. This encourages caregivers to immediately report events and errors by communicating that they will not be admonished or punished. It includes one-on-one meetings in a closed and safe environment and extensive training of the review staff to conduct open, non-judgmental interviews, so that the reviewers can get a deeper understanding of work as performed. The goal is for practitioners to feel safe participating in the review process. RCA^2 addresses this by using repeated language to not blame the frontline practitioner for these events, but to look for more systemic contributors. The CANDOR program addresses this by including formal training for safety reviewers in interviewing techniques, body language, even choice of clothing that the interviewers use.

2.2 Facilitating increased transparency to internal and external stakeholders

Organizational learning, which is one of the four cornerstones of resilience (Hollnagel, 2009), is nearly impossible if newfound knowledge is not effectively disseminated broadly throughout the organization. A lack of available organizational knowledge is one of the common contributors of events that are incorrectly attributed to errors of frontline practitioners (Woods et al., 2010). CANDOR requires that event review materials are available to internal and external stakeholders, including the affected patients and their families. Sometimes this results in increased claims, but it is always the right thing to do, and this is why the organization does it. This creates a partnership with the patient and facilitates better understanding of how work was really performed.

2.3 Valuing firsthand accounts over secondhand accounts

Once an event has been reported, the organization needs to mitigate the risk of falling into the trap of using stale, incorrect knowledge of how work is performed when devising explanations of what happened and potential interventions. CANDOR addresses this by sending reviewers immediately to the location of the incident. Much like the National Transportation Safety Board sends investigators right away to a crash site, it is a priority for reviewers to be present quickly to collect data and accounts that soon after will not be available, or will be distorted. Each person involved is given time for discussion, with a focus on those at the front line. Contrast this to the 'old' way, which often involved recommendations of discipline, counseling, or training of the frontline provider, by panels who *never spoke directly to this provider* during the process.

2.4 Broader dissemination of findings to deliver more sustainable solutions

In addition to making new knowledge available, it must be readily accessible to practitioners when addressing future events (Woods et al., 2010). Both processes address this by actively engaging multiple internal stakeholders at multiple levels of the organization at multiple time intervals. After the reviewers reach consensus on the emerging themes of the case, they communicate with key stakeholders in areas where opportunities for improvement have been identified. In the CANDOR approach, all internal stakeholders come together for a final consensus meeting. They discuss proposed solutions and bring the right leaders to the table. With the involvement of safety scientists who are embedded in the health system, these solutions will often be both sustainable and effective.

2.5 Positive results from these new RCA's

We have seen positive results implementing these new processes at Medstar Health. Because of our size, there are many people responsible for conducting event reviews, and there was wide variation in the way they were done. This was not an immediate change, and there are certainly still some pockets where there is strong influence of the "old RCA" approach. However, we've seen a tremendous movement forward towards a more enlightened approach. People are using the word review instead of investigation, are meeting with involved parties in a one-on-one, non-threatening environment, and have become much more in oriented towards systems thinking. We disclose everything to the patient and family from day one. We support the caregivers involved. And the reviews are performed with a different goal. The review teams know that "nurse error" is not an appropriate conclusion, and they approach with a learning attitude. At time, we still struggle to find the right ways to learn from events and to find sustainable and effective solutions. But when you contrast this with the old method which created a wall of silence, focused on determining blame, and usually closed out without identifying system factors or identifying effective mitigations, this change is a major step in the right direction.

3 PERSPECTIVE 2: THESE AREN'T THE STEPS WE'RE LOOKING FOR

Michael F. Rayo, PhD

It has long been a frustration of the resilience engineering community that the vast majority of safety investigations are conducted with some form of Root Cause Analysis (RCA). Historically, these investigations highlight individuals' mistakes and either miss or underrepresent the system attributes that shaped those individuals' behaviors. However, multiple industries have determined that utilization of the RCA has not improved the safety of their organizations. Many have revised their RCA guidance and have included language consistent with resilience engineering concepts and precepts. However, it is unclear whether these new versions of the RCA move them closer to systemic analyses in any substantive way. As resilience engineering practitioners, how do we know what a step in the right direction looks like?

Observations of complex adaptive systems conducted over the last thirty years have repeatedly reconfirmed that system failures require multiple contributors, which are all necessary but only jointly sufficient (Hollnagel, Woods, & Leveson, 2006). These contributors are often difficult to see, especially during normal work, but can be detected if the investigation explicitly addresses some or all of the following:

1. *Mechanisms*: recurrent general patterns of distributed cognitive work (Woods & Hollnagel, 2006)
2. *Interplay between agents*: interdependency, coordination, synchronization (Woods & Hollnagel, 2006)

3. *Progression over time*: event patterns (e.g., deterioration and recovery) (Woods & Hollnagel, 2006; Woods & Wreathall, 2008)
4. *Pressures*: goal priorities, conflicts, and trade-offs (Woods et al., 2010)
5. *Adaptations*: to gaps/conflicts or opportunities (Hollnagel, 2009)
6. *Emergent*: What emerges from interactions (Hollnagel et al., 2006)
7. *Multi-level*: pressures from the blunt end and external to the system must be understood (Woods et al., 2010)

Recent revisions of the RCA that have attempted to include systems thinking have either unintentionally (or perhaps quite intentionally) misperceived, misunderstood, or co-opted the language of resilience engineering. Ultimately, these new RCA's risk performing the same analyses and coming up with the same conclusions, albeit with different words. In order to mitigate against the risk of inadvertently falling back on previous habits with different labels, updates to RCA's must include the following:

1. Scope of *data collection* is broad enough to reveal the systemic forces that, when understood, rationalize the behaviors of the local agents
2. *Analysis and synthesis* includes abstraction to larger patterns of distributed cognitive work that are associated with system success and failure
3. *Proposed interventions* aim to address systemic contributors over individual causes, and facilitate future proactive learning

In the United States healthcare industry, NPSF and AHRQ have recently released new RCA methods infusing resilience engineering language in the hope of better supporting their goals to ultimately design "effective systems-based improvements to make health care safer" (National Patient Safety Foundation, 2016). Used as examples, they can provide insights as to whether other investigation methods are systemic in how they collect and analyze data as well as propose interventions.

3.1 Data collection: is it broad enough? Are we able to localize local behaviors?

The underlying perspective of an RCA is that safety and performance can be understood by constructing a linear, causal set of events, which leads investigators to the root cause (Dekker, 2013). This inevitably emphasizes the weight of agents and behaviors closest to the sharp end, and deemphasizes the impact of distal systemic contributors derived from forces exerted at multiple levels, both internal and external to the system (Dekker, 2013; Woods et al., 2010). This focus on proximal, sharp end agents begins with what data is collected, and how far into the past is determined in scope for the investigation.

In order to detect the blunt end forces, data collection in systemic investigations include two important aspects. First, investigators directly observe the system to understand how typical work is performed, and how, if at all, the behaviors surrounding the incident were atypical. This is not trivial, because work as performed is different than how work is imagined by remote actors (Dekker, 2013). Second, since observed behaviors are locally rational, even if they are globally maladaptive (Woods et al., 2010), the investigation must increasingly explore events that are further proximal and towards the blunt end to reveal the pressures that rationalize sharp end behaviors.

Although it attempts to deflect blame from sharp end actors, data collection methods advocated by these new methods risk that the investigation will ultimately be prematurely narrow and focused on the sharp end. This is especially true of RCA^2, which continues the use of linear flowcharts to diagram incidents, reinforcing the notion of accidents resulting from a chain of events. Also, even though both CANDOR and RCA^2 emphasizes that investigators get firsthand knowledge about the actors and location of the incident, they do not advocate explicitly seeking out blunt end contributors to the incident, and do not give a recommendation on how to determine how far back in time a review should cover. It emphasizes that reviewers should be looking for systemic issues, but gives little guidance as to how to identify them.

3.2 Data analysis: is it corroborating general patterns of collaborative cognitive work?

Rationalizing local behaviors requires associating them with general patterns of cognitive work. Instead of categorizing actions as right or wrong, which requires hindsight (Dekker, 2013; Woods et al., 2010), they are mapped to patterns of what makes cognitive work difficult. Ensuring these mappings is a safeguard to prematurely closing a line of inquiry or analysis. Researchers have mapped these difficulty patterns to associated macrocognitive functions (Patterson, Roth, & Woods, 2010), the perception-action cycle (Dekker, 2013) and to research-based heuristics (Woods et al., 2010). For example, a nurse not double-checking a patient's medication with a barcode is not determined to be fully understood until its associated patterns are revealed, whether they be goal conflicts (Woods et al., 2010), potential fixation (Patterson et al., 2010), or drift towards failure (Dekker, 2013; Hollnagel et al., 2006). From the published materials, neither RCA^2 or CANDOR encourages this mapping to larger patterns of cognitive work.

3.3 Recommendations: are they targeting the sharp and blunt end? Are they sustainable, or are they susceptible to drift?

Systemic recommendations focus on capabilities that increase the overall system's ability to adapt to future foreseen and unforeseen events. This system attribute has been called adaptive capacity (Branlat & Woods, 2010), margin of maneuver (Stephens, Woods, & Branlat, 2011) and slack (Saurin, 2015; Schulman, 1993). It is preferable that proposed interventions are not extra static resources, but instead are dynamic capabilities that can be accessed either through local or interunit reorganization (Stephens et al., 2011). For example, when car and bus bombings increased in Israel, ambulance drivers drove their ambulances home at night to reduce response time to emergencies (Cook, 2016). This solution was essentially zero-cost and increased flexibility, which made it resistant to future cost-saving measures seeking to redeploy or remove unnecessary resources. From the published materials, neither RCA^2 or CANDOR explicitly encourage these types of recommendations or interventions.

In addition, recommendations focused only on the frontline practitioners and not taking into account the pressures exerted by management and other distant actors will likely not insulate the system from future issues and are more susceptible to future drift towards failure (Dekker, 2013). To its credit, CANDOR shows examples of some of these pressures, although does not provide explicit strategies to address them. RCA^2 does not explicitly address these issues.

4 CONCLUSIONS

Although there is general consensus around current RCA's inadequacies and the benefits of systematic analyses, it is still debatable as to what aspects of RCA reform will drive us towards system thinking, and which will not. On one hand, we must embrace well-meaning RCA changes, even if they do not go as far as we think they should. On the other hand, each of these changes runs the risk of improving small aspects of the overall process without changing the overall tenor of the analyses and recommendations. What's worse, these efforts can lull us into a false sense of security. To compound matters, change in our organizations is slow. We are constantly being asked to predict the future but will not get feedback for years, if at all. It is true that we cannot spend all of our time focused on the negative aspects of new processes that do not fully embrace resilience engineering, but must target those areas that, if changed, will truly make a difference. Hopefully by looking at how these new methods do or do not allow practitioners to see systemic factors we can more expertly focus our attentions where they are best directed.

REFERENCES

Cook, R. I. (2016). Personal communication.

Branlat, M., & Woods, D. D. (2010). How do Systems Manage Their Adaptive Capacity to Successfully Handle Disruptions? A Resilience Engineering Perspective. Presented at the Association for the Advancement of Artificial Intelligence Fall Symposium.

Dekker, S. W. A. (2013). The Field Guide to Understanding Human Error. Ashgate Publishing, Ltd.

Hassall, M. E., Sanderson, P. M., & Cameron, I. T. (2016). Incident Analysis: A Case Study Comparison of Traditional and SAfER Methods. *Journal of Cognitive Engineering and Decision Making*. http://doi.org/10.1177/1555343416652749

Hollnagel, E. (2009). The four cornerstones of resilience engineering, Chapter 6 – pages 117–134.

Hollnagel, E. (2014). Safety-I and Safety-II. Ashgate Publishing, Ltd.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). Resilience Engineering. Ashgate Publishing Company.

James, J. T. (2013). A New, Evidence-based Estimate of Patient Harms Associated with Hospital Care. *Journal of Patient Safety*, *9*(3), 122–128. http://doi.org/10.1097/PTS.0b013e3182948a69

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science*, *42*(4), 237–270.

National Patient Safety Foundation. (2016, January). RCA2: Improving Root Cause Analyses and Actions to Prevent Harm - National Patient Safety Foundation. Retrieved March 29, 2017, from http://www.npsf.org/?page=RCA2

Patterson, E. S., Roth, E. M., & Woods, D. D. (2010). Chapter 14: Facets of Complexity in Situated World. In *Macrocognition Metrics and Scenarios*. Ashgate Publishing Company.

Saurin, T. A. (2015). CLASSIFICATION AND ASSESSMENT OF SLACK: IMPLICATIONS FOR RESILIENCE. Presented at the th Resilience Engineering Association Symposium, Lisbon.

Schulman, P. R. (1993). The Negotiated Order of Organizational Reliability. *Administration & Society*, *25*(3), 353–372. http://doi.org/10.1177/009539979302500305

Stephens, R. J., Woods, D. D., & Branlat, M. (2011). Colliding dilemmas: interactions of locally adaptive strategies in a hospital setting. *4th Resilience …*.

Woods, D. D., & Hollnagel, E. (2006). Joint Cognitive Systems. Boca Raton, FL: CRC.

Woods, D. D., & Wreathall, J. (2008). Stress-strain plots as a basis for assessing system resilience. *… : Remaining Sensitive to the Possibility of …*.

Woods, D. D., Dekker, S., Cook, R., Johannesen, L., & Sarter, N. (2010). Behind Human Error. Ashgate Publishing Company.

SUSTAINED ADAPTABILITY: THE TRANSACTION LEVEL

Jan Maarten Schraagen [1, 2]

[1] TNO, Soesterberg, The Netherlands

[1] jan_maarten.schraagen@tno.nl

[2] University of Twente, Enschede, The Netherlands

[2] j.m.c.schraagen@utwente.nl

Abstract

A new system level, called the 'Transaction Level' is introduced. I argue that such architectures should not be couched in (macro)cognitive terms, but rather in terms of networks of nodes and links that effectuate transactions. The principle of relationality governing this level states that links are selected to attain transactions. The transaction level is a true systems level rather than a perspective on a particular unit of analysis (individual, team, organization). The novelties and advantages of the introduction of the transaction level for the field of resilience engineering are: (1) an increased emphasis on longitudinal data collection and use of social network analysis as one of the tools to analyse data collected on nodes and links; (2) providing an explanation for when transactions fail and may lead to accidents in sociotechnical systems; (3) a renewed emphasis on the study of patterned interactions of sociomaterial assemblages; (4) providing a language for describing architectures for sustained adaptability and thus advancing relative invariants in the study of Layered Networks.

1 INTRODUCTION

Advances in technology and automation have enabled high levels of connectivity, not only amongst individuals, but also amongst teams, organizations and, at global levels, even countries. Networks are a prime example of such highly interconnected units and have been studied as such in a field collectively denoted as 'network science'. From a slightly different angle, a network perspective has been taken in many fields as well, ranging from sociology and psychology to logistics and biology. Recently, in the field of resilience engineering, Woods (2015) has introduced the concept of Layered Networks, referring to the multi-layered character of networks, as well as its numerous interconnections crossing levels.

Layered Networks show 'graceful extensibility' in successful cases of sustained adaptability, that is, these networks have the ability to extend their capacity to adapt when surprise events challenge their boundaries. A key concept in this view is 'adaptation', which includes adjusting behaviour and changing priorities in the pursuit of goals. As surprise occurs continuously, units within the network constantly need to monitor their environment and regulate their resources, in joint coordination with other interdependent units in the network.

Undoubtedly, for both human and artificial systems, knowledge is one of the most important resources adaptive units can bring to bear. Any system that fluently applies knowledge in the service of goals operates at what Newell (1982) has termed the 'knowledge level'. At the 'knowledge level', the principle of rationality applies: if an agent (e.g., an expert) has a goal and knows that knowledge A will bring him or her closer to that goal, then the agent will choose knowledge A. As knowledge is always finite (principle of bounded rationality; Simon, 1955), adaptation can only be local and perspectives of any unit in the network are bounded. In Newell's (1982) terms, the 'knowledge level' is a radical approximation, that is, entire ranges of behaviour may not be describable at the knowledge level, but only in terms of systems at a lower level, i.e. the cognitive level.

However, if knowledge is finite, the only way for Layered Networks to show graceful extensibility is by aligning and coordinating across multiple interdependent units in a network, by shifting and contrasting over multiple perspectives, hence by extending the range of adaptive behaviour of other units. I will argue that this, in effect, calls for a different system level, right above the knowledge level, which I will call the 'transaction level'.

2 SYSTEM LEVELS

There are many definitions of what a 'system level' is. According to Newell (1982), a true system level is a reflection of the nature of the physical world, not simply a level of abstraction. It should be a specialization of the class of systems capable of being described at the next (higher) level. Aggregation occurs within each level and does not take us to the next level on its own; meaning should be added and some things therefore become invisible at the next level (this is another way of saying that phenomena at higher levels have emergent properties). Therefore, although the levels are ontologically irreducible to each other, each level may still be implemented at the next lower level.

Note that this view of system levels is quite different from what we normally take to be 'units of analysis'. For instance, the distinction between micro, meso and macro levels (individual, group, organization) is not a true system level description, in Newell's definition. For instance, Karsh, Waterson, and Holden (2014) proposed 'mesoergonomics' as a way to specify macro- and microergonomic integration. Their aim was to reveal cross-level interactions and to describe relationships between and among levels rather than describing phenomena that emerge from their components but that cannot be explained by them (Hackman, 2003).

Thus, a system level description should be distinguished from a unit of analysis description. For instance, if we take a particular unit of analysis as our focus, let's say an individual, then, from a system level perspective, we could still describe the individual at multiple system levels simultaneously. The individual could be described at a neurological level, at a cognitive level, at a knowledge level, and so forth upward as well as downward (towards the basic particle level). Basically, this conforms to the division of work in science: physics and chemistry deal with lower system levels than psychology and sociology.

It is the goal of science to find invariants in the behaviour it tries to describe. In physics and chemistry, scientists aim for absolute invariants that hold over all stretches of time. When studying artificial (i.e., goal-directed, hence adaptive) systems, such as Layered Networks or in general human-technology-organisation ensembles, these absolute invariants do not hold up. As noted by Simon (1980), adaptive or artificial systems will change as their environment changes. Therefore, it is difficult to discover and verify empirical invariants in these systems, as any laws that govern their behavior must contain reference to their relativity to environmental features. As noted by Simon (1980, p.36) : « It is common experience in experimental psychology, for example, to discover that we are studying sociology—the effects of the past histories of our subjects—when we think we are studying physiology—the effects of properties of the human nervous system ».

Simon goes on to state, however, that we should not despair of finding invariants. Rather than looking for absolute invariants, as the physicists do, cognitive science should search for relative invariants that hold over considerable stretches of time and ranges of systems : « What is invariant in adaptive systems will depend on the time intervals during which we observe them » (Simon, 1980, p. 36). Simon then mentions three time scales on which adaptation takes place : the shortest time scale in which heuristic search takes place ; a longer time scale in which learning (storing and retrieving knowledge) takes place ; and the longest time scale during which social and biological evolution takes place, in the form of discovery of new knowledge and strategies and the transmission of one system to another.

Newell (1982, 1990) has later expanded on this view by taking the time scales Simon (1980) described as his starting point. Newell (1990) distinguished a biological, cognitive, rational, and social 'stratum', each defined by a particular time band during which processes take place. For instance, the typical cognitive processes take place between 100 msec and 10 sec and the typical rational processes between minutes and a few hours. However, Newell (1982) went one step beyond Simon and equated these time scales with system levels that occur in nature (in his 1982 article, Newell confined these system levels to computer system levels, but it became apparent in his 1990 book that he meant these system levels to apply to all biological and artificial systems).

Therefore, system levels should be defined according to the time scales they describe, not to the unit of analysis they describe. The field of resilience engineering studies adaptation of Layered Networks over long time scales (days to years). The relative invariants that resilience engineering hopes to describe are architectures for sustained adaptability. The question then arises what these architectures look like and how sustained adaptability should be described.

3 TRANSACTION LEVEL

Most researchers in cognitive psychology are familiar, albeit implicitly, with the cognitive stratum. Memory search processes take place at this level, as well as some higher-level, but still basic, problem-solving processes, such as building up mental representations and carrying out mental computations. For instance, the description of real-time pilot behaviour when dealing with information presented on displays usually takes the form of a cognitive level phenomenon.

Fewer researchers are familiar with what Newell (1982) termed the 'knowledge level'. This is behaviour at longer time scales. At the 'knowledge level', the principle of rationality applies: if an agent (e.g., an expert) has a goal and knows that knowledge A will bring him or her closer to that goal, then the agent will choose knowledge A. From the outside, the behavior of the expert is highly predictable, once we know the expert's goals and the knowledge that is required to attain those goals. Many studies in resilience engineering in fact take place at this level. Descriptions of how individuals and teams monitor, respond, anticipate and learn usually abstract away from computational limitations and lack of knowledge and rather assume that knowledge is readily available in the service of goals. For instance, in our studies on enhancing resilience in railway teams, Willy Siegel and I have focused on collaboration displays that foster reflection by making implicit knowledge explicit. One such collaboration display is the Resiliencer (Siegel & Schraagen, 2017a). The Resiliencer provides weak resilience signals on performance, workload and safety boundaries of the railway system as well as analysis functions to connect system level signals to personal identifiable details (e.g., a specific train). The application allowed a team of rail signalers to analyse movements toward system boundaries and share knowledge on these movements (Siegel & Schraagen, 2017b). Over the course of our observations, rail signalers increasingly analysed and reasoned about their work. This enriched knowledge beyond procedures, enhancing the ability to cope with the unexpected and unforeseen (Siegel & Schraagen, 2017a). The time scales of our observations was indeed from minutes to hours (after-shift reflections lasted approximately 30 minutes). Also, we looked at the enrichment and exchange of knowledge among rail signalers, which again is a purely knowledge-level phenomenon.

Yet, knowledge-level descriptions have their limitations when we aim at describing architectures for sustained adaptability. Although we analysed the rail signaller's team reflection over the course of a one-week period, we don't know whether their behaviour leads to sustained adaptability, that is, resilient behaviour over longer periods of time. As noted by Siegel in his dissertation (2017, p. 133): "The staff level needs to incorporate the knowledge into procedure updates and take structural actions for the medium and long term, with all the rail parties. This implies an organisational structure change which will influence the evolution of needed skills in the whole organisation and eventually will result in resilience enhancement of the rail sociotechnical system." Yet, the issue is not just one of a difference between the team level and the staff level. As mentioned above, a team could also be observed over a period of months, and a staff could be observed over a period of hours. A unit of analysis (team/staff) is not the defining difference between system levels. What is the defining difference is that meaning should be added to a particular level, which results is some things becoming invisible and other things becoming visible (because of different concepts being used). Hence, as long as we speak of knowledge being incorporated into procedures at the staff level, we are still describing phenomena at the knowledge level. To move to a different system level, we need a different vocabulary.

I now propose that there does exist yet another system level, which I will call the transaction level. It is a true systems level in Newell's sense, that is, it is a reflection of the nature of the physical (and social!) world and not just a point of view that exists solely in the eye of the beholder. It is not a level of analysis that can be applied to any unit of analysis, as, for instance, a network perspective that can be applied to both brains and societies. It is not an aggregation of knowledge, so its behavior cannot be obtained by expanding agents at the knowledge level with simply more knowledge. Rather, no amount of knowledge added will yield the transaction level properties that are characteristic of this level.

A quick overview of the transaction level, in terms of the system under consideration, its components, its laws of composition, its behavior laws and its medium, are in order before entering into details.

The system at the transaction level, the entity to be described, is the network. The system's primitive elements, its components, are nodes and links. Thus, a network is composed of a set of agents and a set of links. The components are assembled into systems by laws of composition that yield strength and reciprocity. The medium at the transaction level is the transaction (as might be suspected). Thus, the network generates transactions by connecting nodes through links. The transactional content may differ widely, from affect and influence to goods and services, and information. Finally, the behavior law, how the system depends upon its components and composition, is the principle of relationality : links are selected to attain transactions. As links are characterized by strength and reciprocity, the generation of transactions is dependent upon link strength and reciprocity.

In contrast to the knowledge level, the concept of 'goal' does not play a role at the transaction level. However, just as with the knowledge level, the transaction level is a radical approximation : entire ranges of behavior may not be describable at the transaction level, but only in terms of systems at a lower level. For instance, the transaction level is poor for predicting how team members that have never met before will interact. It is also poor for predicting the effectiveness of the introduction of a new technology on a person's behavior. However, it is good for predicting the impact of losing someone central to an organization's informal network. It is also good for predicting that a well-established team will exchange relevant information in a timely fashion.

The physical structure of a transaction is filled indirectly and approximately by knowledge systems at the next lower level. This is depicted in figure 1 :

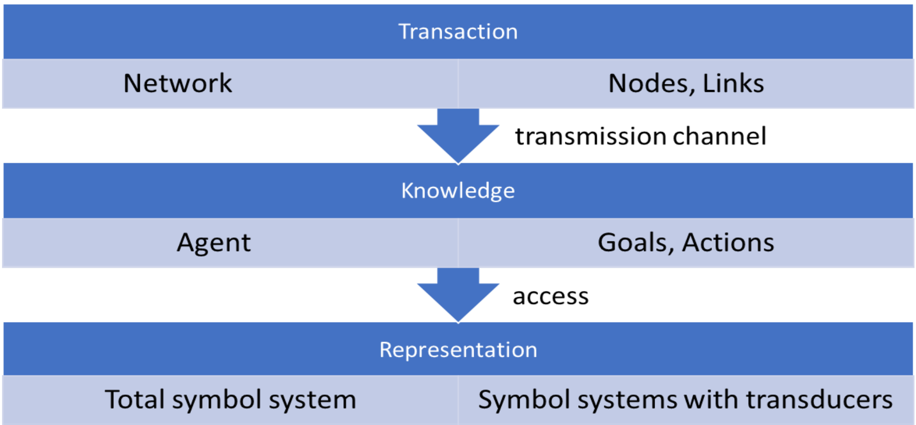


***Figure 1**. Reduction of the transaction level to the knowledge level and the symbol level*

The slogan equation for connecting the transaction level to the knowledge level is: Knowledge = Transaction + Transmission channel. What this means in psychological terms is that humans are social beings that have knowledge of all kinds of possible transactions, but only to a certain extent, due to limitations on communication bandwidth. This knowledge is a person's social capital, or the interpersonal relationships they have with others that enable successful functioning (Hollenbeck & Jamieson, 2015). Social capital is conceptually distinct from the individual-level constructs and it has the potential to enhance prediction of individual and team performance incrementally over those constructs. Social capital information can be quantified using social network analysis (see Schraagen, 2015, for a discussion of the relation between resilience and social network analysis).

4 SIMILARITIES AND DIFFERENCES WITH OTHER APPROACHES

The emphasis on the exchange of transactions between actors in a network is very similar to what Stanton et al. (2006) described in their theory of distributed situation awareness. These authors took a systems level approach and noted that what mattered was that the right information was passed to the right agent at the right time, not that all information is available with a single human agent. Neville et al. (2016) also used the concept of 'transaction' in a similar, though more restricted, way than I do. They referred to transactions as an exchange of situation awareness between agents, which is more than the mere communication between agents. Transactions are enriched by specific and individual interpretations of each agent and so may provide a clue to other agents as to what one individual is working on. As transactions hold the key to safe and efficient performance, post accidents this means that investigators need to understand not only what information was lost but also what transactions were inadequate or were required but not forthcoming (Salmon, Walker, & Stanton, 2016).

However, although superficially similar, Stanton and co-workers' approach differs from my description of the transaction level in several ways. First, although Stanton et al. correctly describe situation awareness as a system level phenomenon rather than an individual level phenomenon, a 'system level' in Newell's sense is not the same as a 'system level' in Stanton's sense. What Stanton et al. are referring to is a difference in the unit of analysis, namely the individual versus the 'system' (where 'system' refers to a sociotechnical system). Hence, in their view, it makes sense to say that a 'system' holds situation awareness or loses situation awareness, whereas in my view, at the transaction level, the concept of situation awareness simply does not exist, as it exists at the knowledge level.

Second, Salmon, Walker, and Stanton (2016), in their application of their Distributed Situation Awareness theory to the Air France 447 accident, focused on the sharp end of the communication patterns of the pilots involved. Again, although valuable, this is a knowledge level analysis rather than a transaction level analysis. What needs to be determined, if we are looking for architectures for sustained adaptability, is what underlying, structural relational patterns were present in the cockpit that led to this specific exchange of information at this particular moment in time. Furthermore, these authors restrict transactions to informational transactions, whereas power relationships and affective relationships also play an important role. Thus, rather than focusing on who said what to whom at a particular moment in time, we should focus on structural affective, power and informational relationships between human and non-human agents in the network.

I agree with Salmon, Walker and Stanton (2016) that failed transactions lie at the root of accidents occurring in complex sociotechnical systems. However, this statement does not explain how transactions fail. The distinction between the transaction level and the knowledge level does at least begin to explain how transactions fail: first, by structural differences in link strength and reciprocity; second, by restrictions on communication bandwidth.

As to the first aspect, one needs to ask whether team members have been able to develop links with each other, and what power relations they have with each other. Of course, as all system levels simultaneously play a role at all times, and the transaction level, just as the knowledge level, is a radical approximation, this implies that, for example, when team members do not know each other well and have not built up structural links with each other, the transaction level is poor for predicting how these team members will interact. We need to invoke the knowledge level in that case to explain absent, inappropriate, incomplete or misunderstood transactions. Invocation of the knowledge level is related to the second aspect, restrictions on communication bandwidth. Even if individual team members possess all relevant knowledge, they may be unable to share all that knowledge, particularly in stressful situations, due to the fact that they can only speak, see and hear so much. A team of experts is not by definition an expert team, if team members don't know when to communicate what information to whom, or don't dare to communicate. This goes back to the first aspect of the establishment of structural and reciprocal links between team members (or agents in general: the interactions between humans and non-humans may also be fruitfully analysed in terms of link strength and reciprocity).
A second field that should be noted is the field of organization studies and the sociology of technology. In particular, Actor-network theory (Latour, 2005) and the concept of 'sociomateriality' (Orlikowski & Scott, 2008) have been highly influential in eliminating the conceptual distinction between humans/organizations and technology. Their view of the social and technical worlds is described by Orlikowski and Scott (2008, . 457) as: "Humans/organizations and technology are assumed to exist only through their temporally emergent constitutive entanglement." As in the transaction level, the principle involved is the principle of relationality and the system to be described consists of 'sociomaterial assemblages'. People and things only exist in relation to each other; in fact, Latour (2005) goes so far as to claim that the distinction does not exist in the empirical world, but rather is an invention by scholars to demarcate disciplines of study. Sociomateriality may be defined then as "[e]nactment of a particular set of activities that meld materiality with institutions, norms, discourses, and all other phenomena we typically define as "social."" (Leonardi, 2012, p.42).

For resilience engineers, the novelty of these approaches lies not so much in the recognition of the importance of technology in the social world, nor even in the recognition that materiality is present in each and every phenomenon that resilience engineers consider 'social'. Rather, the novelty may be in the absolute elimination of any distinction between humans and technology. This is in complete alignment with the description of the primitive elements of the transaction level. The distinction between nodes and links does not make a difference between human nodes and technological nodes. In fact, with the increase in intelligence in technological artifacts, the distinction between humans and technology has already faded. This is not to say that humans and technological artifacts are ontologically identical and indistinguishable. Rather, at lower levels they become distinct entities (perhaps already at the knowledge level, but certainly at the cognitive level). However, at the transaction level, the distinctions are irrelevant.

5 CONCLUSIONS AND IMPLICATIONS

I have advanced the notion of the transaction level as a separate system level directly above the knowledge level. The novelties and advantages of the introduction of the transaction level for the field of resilience engineering are: (1) an increased emphasis on longitudinal data collection and use of social network analysis as one of the tools to analyse data collected on nodes and links; (2) providing an explanation for when transactions fail and may lead to accidents in sociotechnical systems; (3) a renewed emphasis on the study of patterned interactions of sociomaterial assemblages; (4) providing a language for describing architectures for sustained adaptability and thus advancing relative invariants in the study of Layered Networks.

REFERENCES

Hackman, J.R. (2003). Learning more by crossing levels: evidence from airplanes, hospitals, and orchestras. *Journal of Organizational Behavior, 24*, 905-922.
Hollenbeck, J.R., & Jamieson, B.B. (2015). Human capital, social capital, and social network analysis: Implications for strategic human resource management. *Academy of Management Perspectives, 29*(3), 370-385.
Karsh, B.-T., Waterson, P., & Holden, R.J. (2014). Crossing levels in systems ergonomics: A framework to support 'mesoergonomic inquiry'. *Applied Ergonomics, 45*(1), 45-54.
Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press.
Leonardi, P.M. (2012). Materiality, sociomateriality, and socio-technical systems: What do these terms mean? How are they different? Do we need them? In P.M. Leonardi, B.A. Nardi, & J. Kallinikos (Eds), *Materiality and organizing: Social interaction in a technological world* (pp. 25-48). Oxford: Oxford University Press.

Neville, T., Salmon, P.M., Read, G.J.M., & Kalloniatas, A. (2016). Play on or call a foul? Testing and extending distributed situation awareness theory through sports officiating. *Theoretical Issues in Ergonomics Science, 17*(1), 80-103.

Newell, A. (1982). The knowledge level. *Artificial Intelligence, 18*, 87-127.

Newell, A. (1990). *Unified theories of cognition*. Cambridge, MA: Harvard University Press.

Orlikowski, W.J., & Scott, S.V. (2008). Sociomateriality: Challenging the separation of technology, work and organization. *The Academy of Management Annals, 2*(1), 433-474.

Salmon, P.M, Walker, G., & Stanton, N.A. (2016). Pilot error versus sociotechnical systems failure: A distributed situation awareness analysis of Air France 447. *Theoretical Issues in Ergonomics Science, 17*(1), 64-79.

Schraagen, J.M.C. (2015). Resilience and networks. *Proceedings of the Resilience Engineering Association 6th Symposium*, Lisbon, Portugal, June 22-25. Downloaded from: http://www.resilience-engineering-association.org/download/resources/symposium/symposium_2015/Schraagen_J.M.-Resilience-and-networks-Paper.pdf

Siegel, A.W. (2017).Team reflection on weak resilience signals: Resilience enhancement of a rail sociotechnical system. PhD Thesis, University of Twente (CTIT Ph.D. Thesis Series No. 16-416). Enschede: Gildeprint.

Siegel, A.W., & Schraagen, J.M.C. (2017a). Beyond procedures: Team reflection in a rail control centre to enhance resilience. *Safety Science, 91,* 181-191.

Siegel, A.W., & Schraagen, J.M.C. (2017b). Team reflection makes resilience-related knowledge explicit through collaborative sensemaking: Observation study at a rail post. *Cognition, Technology & Work, 19(1), 127-142.*

Simon, H.A. (1955). A behavioral model of rational choice. *Quarterly Journal of Economics, 69*, 99-118.

Simon, H.A. (1980). Cognitive science : The newest science of the artificial*. Cognitive Science, 4*, 33-46.

Stanton, N.A., Stewart, R., Harris, D., Houghton, R.J., Baber, C., McMaster, R., Salmon, P.M., et al. (2006). Distributed situation awareness in dynamic systems: Theoretical development and application of an ergonomics methodology. *Ergonomics, 49*, 1288-1311.

Woods, D.D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety, 141*, 5-9.

RESILIENCE FOR ENGINEERS

John Stoop
Kindunos Safety Consultancy, Spijksedijk 8A, 4207GN Gorinchem, the Netherlands
stoop@kindunos.nl ++31183637484

Abstract

This contribution elaborates on the need to integrate resilience capabilities from the start on into the design of socio-technical systems. Due to their ability to create catastrophic consequences, high energy density systems - such as aviation and railways- should not be measured by the absence or emergence of major events, but by their inherent properties, intrinsic hazards and recovery and resilience capabilities after major events. This contribution advocates the application of systems engineering principles and the revaluation of Good Airmanship as indispensable capabilities to engineer resilience in modern transport systems during design and operations.

1 INTRODUCTION

1.1 A shift in focus

During the last decade a paradigm shift has been observed in managing and controlling safety at both an operational, corporate and governance level from compliance with regulations to competence and continuous improvement of operational excellence (Stoop, De Kroes and Hale 2017).

First, underlying notions of operator's mental models are shifting from a Tayloristic focus on extrinsic motivation, productivity and command/ control strategies of their safety performance towards continual improvement, learning, adaptivity, quality and intrinsic motivation. There is also a shift from a focus on the individual operator and controlling risks to understanding underlying accident causation and systems dynamics on organisational and governance levels.

Second, due to a series of major accidents in high tech industries –internationally in aviation, maritime, railways, process and nuclear power supply- and emergent safety deficiencies in the design and development of major infrastructural projects –in particular in the Dutch railway industry- the focus is no longer solely on the operational phase. A shift is taking place towards design and handling of non-normal situations, aiming at knowledgeable interventions as well as the relative autonomous role of technological development and its interrelations with conceptual change and technological innovation, aiming at the requirements for adaptation at organisational and governance levels.

Third, as a consequence -rather than a static, linear modelling of events and concepts of systems architecture-, a shift in focus occurs towards systems modelling dealing with safe operating states/space models, system viability and recovery, survivability by the ability to respond resiliently to disruptive perturbations. Analysis is shifting towards interactions between external constraints and the configuration and geometry of complex systems throughout their states and phases.

From a systems design perspective, a shift occurs from the performance of the system's components to the performance of the whole system, to oscillation and stability of the Eigenvectors of systems, defining their survivability. Such shifting requires reflection on units of analysis and beyond that, the need to achieve synthesis between components, functions, and values. This is a major engineering design challenge. Current design strategies do no longer suffice at the level of options and opportunities derivate from regular performance, but require disruptive change, technological innovation and adaptation of underlying concepts and notions.

1.2 Resilience engineering

After a period of defining resilience engineering as a concept, identification and analysis of their inherent properties, questions are answered about why resilience is needed and what resilience engineering means in coping with complexity, adaptivity and systems dynamics. A need is emerging to achieve synthesis between contributing disciplines, generalization across application domains in order to make the next step to *how* to enact change, *how* to adapt and innovate in practice based on resilience principles. Such a need is particularly important for change in legacy systems with a global span of control on their networks, markets and social acceptance, in particular high tech industries in the transport domain.

2 CRITICAL TOPICS

Topics that proved to be critical in incorporating resilience in aviation, railways and infrastructure dealt with current engineering design principle in a series of major transport and infrastructural projects in the Netherlands.

These systems are a distinct category of systems, due to their specific technological nature of high energy density systems and their legacy as long lasting entities.

2.1 Emergent criticalities

Emergent criticalities manifested themselves as:

- Transition strategies for deploying technological innovation and cyclic adaptation in the design and development of Schiphol Airport as a major infrastructural hub and implementing ERTMS on the Dutch railway network without serious disturbances or fatal errors in vital subsystems of the command and control systems during the transition period (Beukenkamp 2016)
- The use of survivability as a quantitative measure for resilience in the design and development of in particular the High Speed Line network development in the Netherlands
- Enabling a transition from the human error concept of pilotage to pilotage as a human asset for the design and operations of the 5th generation of commercial aircraft by introduction of Good Airmanship 2nd generation (Mohrmann, Lemmers and Stoop 2015)
- Identification and analysis of intrinsic hazards and inherent properties of high energy density technological systems as a specific category of complex and dynamic socio-technical systems.

These topics aims at:

- cross domain generalization of experiences with engineering resilience in a particular sensitive sector: legacy systems with a global, open network nature, combining a layered structure of a multi-actor involvement in the command and control of such systems and technological components at an innovative level
- development of system control theoretical concepts and models to pro-actively assess the safety of complex systems, both in their adaptive phase to major changes in technology, organisation and governance in early phases of design and development of new disruptive technologies, business models and market conditions.

Due to their already non-plus ultra-safe performance and expectations of a public confidence and risk acceptance nature, such systems require a dedicated design and engineering methodology with quantifiable safety requirements and performance indicators at a systemic level. Such design and development requires an upgrading of the man-machine interface from an either/or level towards a higher unit of integrated M-M-I analysis, combined with constraints of both external and internal natures.
The approach is based on combining concepts of control theory, systems engineering, resilience engineering and safety investigation. The approach has potential for design and development of new technologies, in particular in the transport domain.

2.2 Inherent properties

In analysing complex and dynamic systems, safety is frequently considered an emergent property, to be disclosed in its actual performance during operational practice. In this contribution, we argue that safety is primarily an inherent property, defined and designed into systems from the conceptual phase on. Historically, safety in complex transport systems are defined by their accident and incident frequency and the unacceptability of major disruptions and catastrophes in the functioning of these public transport systems. Due to the decrease of accident frequency, the physical damage and injuries to users are challenged as an appropriate measure for their safety performance. Instead of looking what went wrong, we should shift to analysing what went right and adapt to a proactive perspective. This proposition of abandoning retrospective approaches in favour of prospective approaches is challenged from an engineering design perspective. Safety performance in complex systems is both determined by their societal goals and values, design principles, intrinsic and inherent properties and emergent operational performance from both a feedback and feed forward perspective. This contribution elaborates on the architecture and configuration of complex and dynamic systems, elaborating on their technological intrinsic hazards, multi-actor characteristics, business models, hierarchical control mechanisms, institutional arrangements, adaptive potential and network configuration dynamics. Several case studies in aviation and railways demonstrate that safety performance indicators can be traced back to each of such systems characteristics. They enervate the assumption of a linear, direct relation between safety performance, traffic volume and growth.
To this purpose, this contribution elaborates on the variety of modelling techniques and network typologies which are available for providing structure to understanding the dynamics in complex systems and the multiplicity of system states that are potentially available. Analysing the nature, tractability, stability and

resilience of these states determines whether a system remains controllable and manageable across the variety of operating envelopes and transitions across these envelopes. This contribution demonstrates the validity of the notions of inherent properties and system states by case studies from the aviation and high speed line railway industry.

3 SOCIO-TECHNICAL SYSTEMS BY DESIGN

Socio-technical systems must first and foremost be safeguarded by design due to their specific characteristics as a distinct category of high energy density complex systems. From a social perspective there is a conscious and multi-actor involvement in the optimization of conflicting values, goals and primary production processes. From a technical perspective, they may result in unacceptable catastrophic physical consequences by an instantaneous, unanticipated and uncontrolled release of high levels of energy of a mechanical, chemical or nuclear nature. They adapt to change in their operating environment by deliberate, disruptive and innovative changes in technology, organisation and governance. A proactive assessment of their safety performance is imperative to prevent unacceptable emergent behaviour and catastrophic consequences. The management of the total energy that is stored in the system is a challenge that must be controlled proactively throughout all system states, mission phases and operating constraints.

3.1 High energy density systems

Due to the increase in size and scale of modern socio-technical systems, the uncontrolled release of energy can result in catastrophic material consequences and loss of all lives of a large population at risk, both inside and outside a system. The total energy stored in complex systems can be expressed in Megawatts as the sum of its kinetic and potential energy. The energy content of a High Speed Train and a Jumbo jet can be compared to a nuclear power plant, as depicted in table 1.

	weight	speed	altitude	Energy/sec
High Speed Train	430 tons	250 km/h	ground level	1053 MW
		320 km/h	ground level	1740 MW
A380 Jumbo jet	MTW 575	900 km/h	10.000 m	75 000 MW
	at take-off MTOW 575 tons	260 km/h	ground level	1500 MW
	at landing MLW 386 tons	260 km/h	200m above ground level	1252 MW
Nuclear power plant	Average size			800 MW
	Borsele (Neth)		Sea level	450 MW
	Chernobyl		Sea level	600 MW
	Fukushima		Sea level	784 MW

Table 1 Total system energy content

Such a total energy management strategy is interesting in particular in aviation with respect to the balance between kinetic energy due to the airspeed control and potential energy due to the altitude and attitude control. The total energy of an aircraft has to be controlled and dissipated back to zero in order to bring the flight to a safe end. This kinetic and potential energy distribution varies across the various flight phases. The total energy of an Airbus A380 in cruise flight is about 75000MW. This amount of energy is the sum of 18700 MW of the airspeed (Mach 0.85) and 56400MW due to the cruising altitude of about 11000m. This means that the energy balance management in this flight phase is based for 25% on the speed control and 75% on the altitude and attitude control. During landing, the kinetic energy reduces to 1006 MW at 260 km/h minimal landing speed at Maximum Landing Weight MLW of 386000 kg and the potential energy to 246 MW at the Maximum Landing Weight at 200 feet over ground level, the go-around decision height. The total energy during landing is about 1252 MW. The potential energy at 200 feet altitude in final approach is reduced from 75% at cruising altitude to 19.6% of the total energy content. The energy ratio management changes towards a predominant control over speed and attitude.

3.2 Multiple performance indicators

Historically, safety in aviation is not only expressed in achievements and policy targets but also in technical airworthiness requirements. Taking into account that zero risk is unachievable in any human activity, acceptable safety target levels had to be established in the perspective of an unbalance between safety and expected growth (Hengst, Smit and Stoop 1998). An array of potential units for measuring risk can be used, discriminating *relative* safety related to the traffic volume and *absolute* safety, related to the annual number of fatalities. Differences across fleet segments and services, scheduled, non-scheduled flights and general aviation, accident rates per aircraft class and world region, as well as life expectancy of aircraft have to be taken into account because risk acceptance by the general public and personal appreciation of risk depends on convenience and pleasure in the various types of private and public risk taking activities. For each activity, a unit of measurement has to be selected since it makes a large difference whether safety is related to the absolute number of fatalities, a critical flight phase or the distance and time flown. For *air services*, as the criterion for safety performance the fatality rate per passenger km is used, while for *airworthiness* the level of safety is expressed per aircraft hour of flight. These two criteria are related by the number of passengers per aircraft, the survivability rate per aircraft and the blockspeed of the aircraft (Wittenberg 1979):

- Number of passengers km P
- Aircraft flying hours U
- Aircraft flying kilometres S
- Assuming K passenger fatalities in R fatal accidents, the fatality rate per passenger km is K/P and the fatal accident rate per flight hour R/U.

For the relation between these quantities holds:
Eq (1) $K/P = R/U*K/R*U/P$
In this expression are introduced:
$k = K/R$ = average number of fatalities per fatal accident
$p = P/S$ = average number of passengers per aircraft
$V_B = S/U$ = average block speed
Then for equation (1) can be written:
Eq (2) $K/P=R/U*k/p*1/V_B$

Or in words: Pass.fatalities/pass.km = fatal acc./flight hours *fatal per acc./pass per aircraft*1/blockspeed. This dimension analysis shows that the introduction of long haul flights, increased survivability rate per accident, increase in blockspeed and larger aircraft have had a major influence on the decrease of the fatality rate per passenger km.
In addressing the issue of acceptable safety levels, two assumptions were made:

- With the expected increase of traffic volume, safety levels may not fall below the achieved levels for reasons of public acceptance
- The level of growth is linear related to the number of accidents.

In socio-technical systems with a high safety performance level, such as aviation and railways, these assumptions proved to be obsolete due to the non-linearity of complex systems and changes in public safety perception and appreciation.

3.3 Changes in system performance indicators

Business models and earning systems as incentives for efficiency versus thoroughness trade-offs are very powerful drivers for cost-efficient operations. In modern business concepts, calls for lean production, faster, cheaper and better performance are frequently heard.
With the introduction of New Economy principles in the transportation sector, three simultaneous developments have changed the drivers for cost-effective decision making. Changes in economic and logistic infrastructures, safety philosophy and selection mechanisms for preferential solutions have shifted from safety performance criteria towards exploitation, availability and cost-efficiency criteria. Cost-benefit considerations and environmental constraints in operations have become dominant. Instead of covering technical deficiencies by an array of technical provisions, a 'willingness to pay' and cost-effectiveness of solutions have become prevalent. Other arguments than safety have to been taken into account in decision making.
Differences in expertise are considered hindrances or even unjustifiable instruments to control the outcomes of a consensus process. Such an environment of 'participative policy making', assumes equality between parties and change the role of experts. Public private partnerships are favored as an answer to hierarchical ordered governmental projects on major infrastructural projects in tunneling, railways and aviation. Safety becomes a 'social construct' instead of an outcome of objective assessment based on professional experiences, quantifiable performance parameters and expert opinion. Such a 'new approach' in safety thinking shifts the focus towards

prevention, flexibility, cost-benefit considerations , quantification of key performance indicators and institutional arrangements. This 'new' approach is a response to the inadequacy to provide substantive progress in conventional safety in the context of a 'new economy' context. Implicit assumptions are that the market should be best prepared to bear the risks and supply the knowledge, while a process approach should drive out substantive approaches. Private parties should not be disturbed by approval of their technical solutions, but should have their hands free to inform government about their selection of preferential solutions. Performance of a systems is reduced to measurable and quantifiable performance indicators. Safety is not such a parameter. Such a regime may reduce or improve the overall safety performance level of a system.
In comparing similar concepts, two options emerge:

- a low systems safety level, characterized as a earning system. In such a system, liability issues, blame and performance are pivotal. Willingness to pay and ALARA techniques prevail, while rule compliance and inspections are important control mechanisms. Safety is controlled at the organizational and company level.
- a high systems safety level, characterized as a learning system. Such a level is guaranteed by quality performance, transparency, communication and cooperation. Sharing responsibilities and information is essential for common learning and indirect cost are recognized. Responsibilities and roles are guaranteed by institutional arrangements.

In selecting either of such options as preferential, specific criteria should be available. Identifying systemic values in a multi-agent based environment has become a topic.

4 PREREQUISITES FOR ENGINEERING RESILIENCE

4.1 Towards a systems engineering perspective

The percentage of the total growth of the traffic volume expressed in passenger km must be compensated by an equivalent decrease in percentage of the fatality rate per passenger km. In the past, safety improvements have been accomplished pragmatically changes in technology, aircraft operations and ground equipment. These achievements have been a combined effort of all parties involved: manufacturers, airline operators, authorities and research institutes.
Advocating a more rational tool for establishing a safety level -such as cost-benefit analysis- such approaches are confronted with hardly comparable costs for value of life, operating costs and cost for safety investments. While costs of individual accident are relative low on a sectoral level of costs, the overall safety enhancement measures following from such accidents may be excessive for the sector. A target safety level for aviation based on a rational cost-benefits approach seems hardly achievable (Wittenberg 1979).
Consequently, another approach has to be favoured where likely improvements can be obtained: the analysis of aircraft accidents and the identification of their causes. A distinction is made in two principal categories in this analysis of aircraft accidents: accidents occurring during normal flight conditions, attributable to a lack of airworthiness and operational factors, and accidents during non-normal flight conditions such as due to human factors, either flight crew, ground personnel or weather conditions such as turbulence. Historically, two practical, operational areas for improving air safety have been applied (Wittenberg 1979):

- The human factor. The predominant position of the human factor as an accident cause only partly can be contributed to direct fault in the performance of the flight crew. The human error is compounded by deficiencies in the design due to a lack of human engineering or by inadequate training for the job to be performed.
- Classification of events by primary production functions, flight phases and system states. Improvements of equipment and procedures for aircraft navigation and air space control will be required to cope with the increase of air traffic in the future. Areas with already dense traffic flow - in particular in the Terminal Movement Area- will benefit from congestion and conflict handling measures.

More rational approaches had to be developed in the 1970's for the introduction of civil jet aircraft and new technologies such as the supersonic Concorde and Automated Landing System development. The allowable probability of failures is inversely related to their degree of hazard to the safety of the flight. No single failure or combination of failures should result in a Catastrophic Effect, unless the probability can be considered as Extremely Improbable, in effect lower than 10^{-7}. Interesting in this approach is the total amount of flight hours per year that are produced by the aviation industry as such. Only a few aircraft types can surmount the 10^{7} requirement, accumulating sufficient flying hours. Consequently, accomplishment to the overall safety target of the airworthiness code *can never be proved by actual flight data* but should be settled by a System Safety Assessment approach. Due to the effect of the increase of aircraft speed and aircraft size, the passenger fatality rate expressed per passenger km has decreased in the past far more than the fatal aircraft accident rate per flight hour. In the coming decades, the favourable effect of increasing aircraft speed and increasing aircraft size will no longer occur. This parameter analysis demonstrates that changes in aircraft size and long range flights had an impact on the improvement factor required for the fatality rate per *passenger km* versus the fatal accident rate based on the *aircraft flying hours.* Consequently the adoption of this new rationalized safety approach severed the assumption of a linear relation between accident rates and traffic growth. As a consequence of the return to smaller aircraft after the jumbo jet era and the very high survivability rate, a shift in safety focus occurs from aircraft design parameters to operational parameters and other primary system components; airports and ATC.

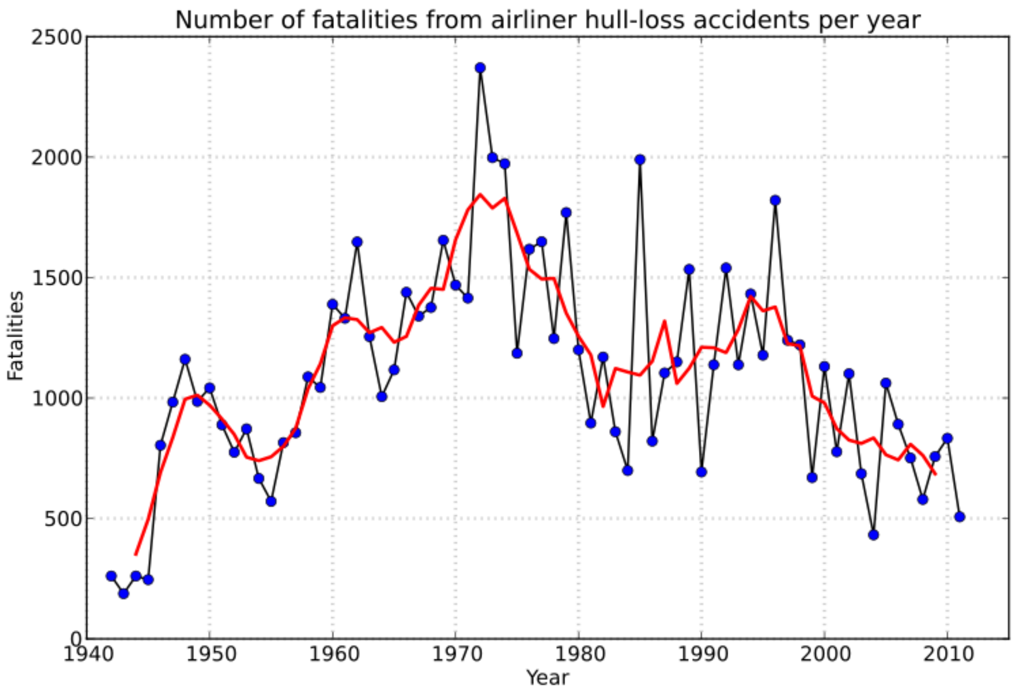


Fig 1 Non-linearity between safety performance and growth

The FAST (Future Aviation Safety Team) and CAST (Commercial Aviation Safety Team) projects in the EU and USA serve to improve the aviation safety level in passengers fatalities per passenger km, to compensate the increase of the transport volume in passenger km of the 1990's (FAST 2014). Simultaneously, the introduction of glass cockpits, pilot information processing and decision making support systems and satellite support facilities for flight crews and ATC each have had their share in the safety enhancement of commercial aviation. A transition to a safety assessment of the overall aviation system is under way: focusing equivalently on the three main components aircraft, airport ant ATC throughout their operational processes. The architecture of systems becomes a focal point of concern.

4.2 Towards a systems architecture

By identifying four dimensions of a system, a problem can be approached from different viewpoints by making a number of 'cross sections' through a problem. If these cross sections are properly chosen, each cross section shows different 'dimensions' of the problem. Such a structured search is referred to as the 'dimensions' technique (Stoop 1990). The objective of the 'dimensions' technique is to establish a description of the problem in the context of a socio-technical system which makes a reference to the life-cycle, dynamics and structure, culture, context and content the relevant system dimensions.

The 'dimensions' are respectively:

- historical: this dimension provides insight into the development of the problem and the long-term development of its technical, organizational and social factors and hence, of the controllability of the problem in the context of the long term development of the system. This dimension covers the Context of a system

- life-cycle: from design, development, manufacturing, through us towards demolition. This dimension gives insight into the feed-forward and feed-back coupling of knowledge and expertise between system phases and knowledge about the criteria relevant for improvement and change. This dimension covers the Structure of a system
- process: this dimension gives insight into the 'normal' use of the system and describes the content of the processes that occur in 'normal' functioning. It gives insight into the tasks, activities, procedures, tools, equipment, operating environment, inputs and outputs of the system. This dimension covers the Content of a system
- culture: this dimension characterizes the system as occupational, transport. leisure or domestic. It gives insight into the (social) objectives, of the system, the role, positioning and functioning of stakeholders, their views, norms, values and codes of conduct. This dimension covers the Culture of a system.

The 'dimensions' technique collects data from normal as well as disturbed functioning, addressing all available performance indicators from intended and actual use and develops from broadly descriptive towards detailed explanatory. Data collection can be conducted by literature study, interviews, document analysis, on-site investigation and other forensic techniques.

The four dimensions are explored in parallel and should result in credible, plausible and verifiable description of the problem under scrutiny in its systemic environment.

4.3 A system life cycle approach: the DCP diagram

In order to integrate safety in design and operations, a new notion of vectoring safety through the systems landscape should be defined. Such a notion consists of three principal elements, being Design, Control and Practice (DCP). They can be interrelated along three dimensions, being a systems approach, a life cycle approach and a design approach. Together they constitute an integrated systems architecture prototype: the DCP diagram.

A systems dimension defines three levels: the micro level of the user/operator, the meso level of organization and operational control and the macro level of institutional conditions.

The life cycle dimension defines a series of subsequent phases, being design, development, construction, operation and modification. At this dimension, the coordination of decision making among actors across the phases is crucial.

The design dimension identifies three principal phases in design, being goal –expressed by a program of requirements, concepts and principles-, function –expressed by design alternatives- and form, expressed by detailed design complying with standards and norms. At this dimension, the potential of technical innovation for new safety solutions is crucial.

The operational dimension. Eventually, only in practice safety is visible and actual consequences of accidents occur. At each of the other levels and phases however, separated in time or space, safety critical decisions have been made by different actors. The diagram demonstrates who, how, at which moment can contribute to safety and risk assessment

To manage consequences of new technology and innovation in transport systems engineering design, three principal lines are available:

- the Practice-Control line. Along this line, an upgrading in interventions takes place. The focus shifts from the performance of individual operators towards the meso level of organization and management in allocating resources, skills, operating procedures and responsibilities. At a macro governance level, rules, regulations and legislation, inspection, certification and governance oversight are addressed as safety enhancement opportunities.
- the Design-Control line. Along this line, decision making and safety assessment methods and standards should be elaborated, to facilitate coordination among stakeholders and actors, participating in major project developments. Several initiatives have already been taken such as safety impact assessment techniques, harmonization of standards by drafting EU Guidelines and Directives on specific topics such as tunnel safety, land use planning or external safety.
- the Design-Practice line. Engineering design methods for integration of safety in technological innovation are in their earliest phases of development. Historically, an impressive variety of design techniques is

available. However, these instruments focus on specific industrial sectors and detailing levels of engineering design of components and are not always generically applicable across modes, disciplines or sectors.

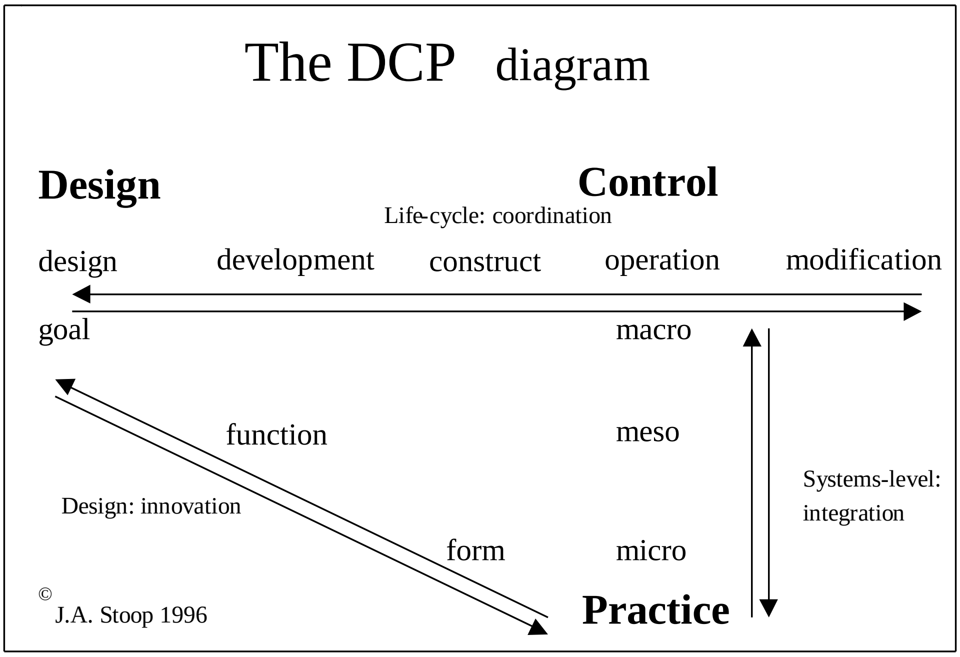


Fig 2 The Design, Control, Practice diagram

In order to design a coherent system and to maintain oversight over the system functioning, a system safety integrator role should be defined. During the design of complex transport systems, a dedicated responsibility should be allocated to assure continuous monitoring of the safety aspects along both lines during its design.

Abolishing obsolete safety constructs

To the purpose of a scientific safety analysis of recovery and resilience capabilities, it is inevitable to abolish three obsolete constructs that have dominated the debate on safety investigations:

- Probable cause, to be replaced by plausible scenario descriptions
- Human error, to be replaced by the notion of reasonability of responses
- Accident modelling, to be replaced by investigative event reconstruction.

The first two constructs have a history as judicial and psychological construct and are frequently criticized for their theoretical and practical applicability during investigations. Such criticisms are mainly based on experiences in the process and nuclear power industry as stationary and hierarchical organized and managed corporations and small and medium enterprises with simple and less complicated events. In major investigations in the transport industry -in particular in aviation and the maritime-, scenario descriptions and reasonable responses have a legacy in accident prevention and Good Airmanship/Good Seamanship.

The construct of reasonability of responses has a history in tort law and disciplinary law, in assessing professional conduct and ethics. This construct became disconnected from safety investigations with the introduction of blame free and preventive investigations and has to be re-introduced in the framework.

5 GOOD AIRMANSHIP

Towards a human habituated response

In cognitive modelling of pilot behaviour, the common reductionist paradigm is to deal with the pilot as a rational, knowledge based and informed decision maker. Many decisions and actions however are routine based, executed at the skill and rule based level of cognition. Such responses are trained, engrained and maintained by simulator training, recurrence and proficiency checks, line checks, incident reporting and audits. Decisions and actions however are not only rational. Since the research of Pavlov, the importance and impact of intuitive, emotional, conditioned and subconscious responses is recognized. Conditioned, automatic responses are predisposed responses based on expertise, competences and previous experiences. The rationalization of such decisions, actions, reasoning and motives remains speculative until after the actions. In general, operators trust on their experiences with similar problems. Their trust and experience will lead to 'automatically' right decisions and actions, compliant with expectations. The reasons for such performance can only be retrieved in hindsight by observations, interviews, recorded conversation and re-enactment of the action sequence. The role of intuition, instinct, reflexes, predisposition, beliefs and emotions is obscured until the actual outcome of the actions (Mohrmann, Lemmers and Stoop 2015).

In analysing a series of accidents, Den Hertog and Roelen (Den Hertog 2011) posed the question why well trained and experienced pilots with high qualifications could fall into a trap of formally incorrect responses to emergent safety issues.

They clarified a recurrent chain of events in which managing concomitant abnormalities and prioritization of event handling lead to the detriment of a safe flight performance, induced by the fact that they were primed due to prior events in their problem solving process.

Such a chain of events that becomes safety critical, contains a succession of an aircraft malfunction, an abnormal situation and unusual conjunction of conditions, decisions and actions that, if they were to occur individually, are relative benign. The accidents arose out of usual human performance in unusual circumstances (Den Hertog 2011).

The components of such a chain repeatedly consisted of:

- A technical malfunction which unanticipated interacted with other system components
- Creating multiple phenomena simultaneously of a relative benign nature
- While in a stressful situation, mutual reliance on crew competences in a professional environment
- Primed with problem solving of prior events
- Deprived the crew from recognition of the actual system state and situation.

In these accidents a combined occurrence of technical failure, automation surprise and flight performance collapse created an aerodynamic stall which became unrecoverable. Successful recovery in such situations does not rely on better training or enhanced flight deck design, but on the available time, resources, information, recovery options and regaining control over the situation. Such situations have been demonstrated to be survivable, even beyond expectations, by the A300 Bagdad missile attack, the US 1549 Hudson ditching and the Qantas A380 recovery to Changi Airport. In these situations, the ability to generate new options beyond regular trained situations contributed to the recovery of the situation.

In the analysis of habitual responses, the perspective of a conventional human performance analysis is abandoned. Instead of asking the question why the crew deviated from regular performance, the question is posed: why did their performance make sense to them at the time? A better understanding of human behaviour and decision making under stressful situations, unusual conditions and habitual responses can assist to improve flight training and flight deck design.

Such understanding requires the abolition of conventional notions because they proved to run short in providing a satisfactory explanation of the event and intervention in the situation:

- No proximate or remote cause was established
- No critical human error was identified as a satisfactory explanation of the event
- No accident models could have grasped the phenomenon with respect to the habituated responses that were identified in the investigation.

The debate on erroneous pilot responses to system malfunctioning frequently refers to situation awareness and automation complacency in complex socio-technical operating environments. The issue of habituated responses and successful recovery addresses a much wider range of operator's responses, irrespective of technological complexity or transport sectors. It has a long history in the maritime, aviation and railway sectors.

In the early 1960's, the Dutch Railway Investigation Board introduced the issue of reasonability of responses formally in her working procedures in order to learn from the practical experiences and expertise of train drivers (De Kroes 1996). Board members had unrestricted access to train drivers -not only those involved in accidents- and were allowed to observe train drivers in their daily work and interview them accordingly after their trips. This made it possible to ask why it was reasonable for these operators to decide and act as they did. Such an approach provided a timely and direct access to train driver perceptions and decision making both in regular and safety critical conditions. This approach was later internationally published and made accessible for academics in a popularized version by Sidney Dekker in 2005 with his seminal book *Ten Questions about Human Error.*

6 CONCLUSIONS

Based on our experiences with major transport and infrastructure projects in the Netherlands, in this contribution we have identified a specific class of socio-technical systems: high energy density systems. To enable recovery and resilience in such systems, such capabilities should be designed into these systems as inherent properties.

Measuring the safety performance of such systems cannot be restricted to a fatality or injury rate as manifested during operations, but also should take into account characteristics of the primary processes-such as services provided and service worthiness- and economic drivers for change and their underlying business models. This requires a shift towards a system engineering from both a Design, Control and Practice perspective.

Finally, several dominant but obsolete safety constructs have to be abolished in order to facilitate a shift to integrating resilience into the design process at the system architecture level. To this purpose, in particular a shift from 'human error' to a habituated and intuitive Man-Machine-Interaction level is indispensable.

REFERENCES

Beukenkamp W., (2016). *Securing Safety*. Doctoral Thesis Delft University of Technology.

Dekker S., (2005). Ten questions on human error. Ashgate

De Kroes J.L., (1996). *Slachtoffers.* Valedictory Lecture, Delft University of Technology.

Den Hertog R., (2011). Two accidents analysed another way. 'Free will does not exist'. Future Aviation Safety Team presentation November 2011.

Hengst S., Smit K. and Stoop J., (1998). *Second World Congress on Safety of Transportation*. 18-20 February 1998, Delft University of Technology. Delft University Press

Mohrmann F., Lemmers A. and Stoop, J., (2015*) Investigating Flight crew recovery Capabilities Regarding System Failures in Highly Automated Fourth Generation Aircraft*. Aviation Psychology and Applied Human Factors 2015, Vol 5(2) pp . 71-82

Stoop J., De Kroes J. and Hale A., (2017). *Safety science, a founding fathers' retrospection*. Safety Science 94 (2017) 103-115

Wittenberg H. (1977). *Safety in aviation; achievements and targets*. Technische Hogeschool Delft, Lucht- en Ruimtevaarttechniek. Memorandum M-353

MODELLING ORGANIZATIONAL LEARNING FROM SUCCESSES IN THE NUCLEAR INDUSTRY –STAFF MEETINGS AS FORUMS OF KNOWLEDGE SHARING AND ACQUISITION

Kaupo Viitanen [1], Hanna Koskinen [1], Ann Britt Skjerve [2], Christer Axelsson [3], Marja Liinasuo [1] and Rossella Bisio [2]

[1] VTT Technical Research Centre of Finland LTD, P.O. Box 1000, FI-02044 VTT, Finland

[1] kaupo.viitanen@vtt.fi

[2] Institute for Energy Technology, Norway

[3] Vattenfall AB, Sweden

Abstract

Utilizing lessons learned from successful experiences in the context of safety-critical organizations has been receiving increasing interest among both scientific and practitioner communities. However, despite the attention, there is a need to better understand how success-related knowledge can be utilized to ensure safety and what tools and practices can be used to facilitate this process. In this paper, we focus on staff meetings as forums of knowledge sharing and acquisition. We describe staff meeting practices from empirical case studies, carried out at two Nordic nuclear power plants, and examine how the staff meetings contribute to organizational learning from successes. Based on these insights, we propose an integrative framework that aims to identify the factors that facilitate or hinder organizational learning from successes.

1 INTRODUCTION

During the past decade, there has been a growing interest in utilizing lessons learned from successful experiences to ensure safety. In the scientific community, the Resilience Engineering research tradition has put effort on providing an alternative approach to safety management for high-risk industries. For instance, Safety-II (i.e., ensuring that things go right) emphasizes understanding successes as a basis for ensuring safe activities (Hollnagel, 2014). The general ability to learn has also been established as one of the cornerstones of resilience (Hollnagel, Pariès, Woods, & Wreathall, 2011). In the practitioner community, interest in successes is reflected, for example, in the nuclear industry Operating Experience guidelines (e.g., IAEA, 2008), local initiatives in some nuclear power plants (NPPs), and in the institutionalized practices of collecting and sharing industry best practices by umbrella organizations such as WANO.

Organizational learning refers to the creation, acquisition and sharing of knowledge between the organizational actors, and acting upon it (e.g., Garvin, 1993). In order to avoid the accumulation of success-related knowledge (i.e., what success took place, and how) only in individuals, it is important to ensure that the organizational structures and learning processes that relate to successes exist and are effective. However, there are challenges in organizational learning from successes. For example, success-related knowledge does not naturally mobilize institutional processes, tends to get stored in individuals or in non-codified structures and thus might not get shared with others in the organization (Madsen & Desai, 2010; Viitanen et al., 2016). Therefore, there is a need to understand how success-related knowledge is managed in organizations and what tools or practices can be used to facilitate this process.

We define *success* as exceeding, matching or returning to an expected level of performance (Viitanen et al., 2016). Expected performance is understood loosely here and can include, for example, safety as measured by leading or lagging indicators, or performance as measured by traditional project management measures such as schedule, cost and scope. This definition results in three types of successes: *extraordinary successes* that are characterized by exceeding the expected performance (e.g., creating new practices or processes, or improving the existing ones); *normal successes* that are characterized by matching the expected performance (e.g., daily routine work, nothing out of the ordinary appears to happen); and *recovery successes* where the performance returns to the expected level (e.g., recovering from adversity, solving problems, repairing broken equipment). We have found that extraordinary successes are most likely to be acknowledged and noticed, while normal successes remain mundane and are thus often ignored; recovery successes – while potentially noteworthy – are also frequently neglected because the failures or breakdowns that led to the adverse event usually take precedence in terms of attention (Viitanen et al., 2016).

This paper is based on the findings from our ongoing study (for further details see Viitanen et al., 2016) where we aim to provide insights into how successes can be identified and utilized for learning purposes in the nuclear industry. We conducted a literature review and theoretical work on the concept of ”learning from success”, and two empirical case studies at Nordic nuclear power plants to identify successes, lessons learned, and the learning practices utilized. The analysis of the empirical data revealed that a multitude of tools or practices exists that either can be used or are already used at the NPPs for the purpose of learning from successes (e.g., staff meetings, information and reporting systems, newsletters, bulletin boards, emails, training sessions). In this paper, we will not report the study in its entirety but rather focus on staff meetings as a tool for enabling organizational learning from successes. Staff meetings are chosen due to their apparent prevalence and potential usefulness for various knowledge management functions, including knowledge acquisition and sharing (e.g., identifying and reflecting successful experiences), knowledge creation (e.g., joint innovating) and storage (e.g., minutes of meetings). For this paper, we analysed the data collected in interviews, field observations and workshops with plant personnel with a focus on identifying the factors that influence the realization of these functions. In this paper, we will present the main findings from the analysis of staff meetings and propose an integrative framework that aims to help identify the factors that facilitate or hinder organizational learning from successes.

2 EMERGING THEMES

When we discussed the viability of including success-related items in staff meetings (e.g., attempt to capture successes after a task, identifying and sharing insights from past successes, etc.) with the interviewees, the following main themes emerged. First, the *cultural influence* on sharing success-related knowledge was underlined. For instance, several interviewees found that making a big deal of one's own successes is frowned upon within their culture. It was also implied that culture may have an effect on receiving feedback. Especially in situations where positive feedback is given in the presence of the whole group feedback, it may be perceived as uncomfortable. In fact, one of the supervisors we interviewed suggested a "de-personified" approach to sharing successes: avoiding discussing the individual's actions but instead focusing on the practices utilized in the particular situation. In addition, if a success was presented and attributed to individual excellence, this was believed to result in negative atmosphere in the group. A potential workaround for this was noted by one of the experts who commented that individual successes are typically discussed with the immediate supervisor rather than the whole group. Another potential workaround mentioned was that the successes are highlighted by someone else (i.e., a "proxy") instead of the first-hand succeeder. Personification of successes was thus clearly seen an issue and something to avoid in this particular NPP. On the other hand, several interviewees brought up the potential usefulness of promoting successes for *motivational* purposes, which leads to a difficult dilemma for organizing staff meetings: how to promote the successes of the succeeders without offending the others? The cultural influence was most often attributed to national culture by the interviewees; however, we hypothesize that other cultures, such as micro-cultures within teams or departments may also play a role. These findings resonate with previous literature on the influence of culture on knowledge management, which, for example, highlights culture as a context for how knowledge is created, shared and used (e.g., De Long & Fahey, 2000).

Secondly, we observed that promoting learning from successes may benefit from *contextualizing the concept of success*. While this theme was not explicitly mentioned by the interviewees, context seemed to be an important underlying factor influencing the way in which they viewed the concept of success. We found that the interviewees from various departments defined success in their work quite differently – undoubtedly due to the different objectives and environmental characteristics of their tasks, and the problems they cope with in their work. For instance, an IT expert related success to troubleshooting (i.e., "recovery successes") and mentioned that their practice of discussing solutions to fault conditions in group meetings is a natural way of sharing successes – he contemplated that re-labelling this practice as "learning from successes" might not make sense to the group. This relates to a third emerging theme, which was the notion that success items should, if possible, be *naturally integrated* into existing meeting practices to be accepted. Another interviewee pointed out that a structured sharing of successes in meetings might not be a good idea because it would be perceived as artificial. This interviewee thought that if the success item was perceived as an "authentic" part of the everyday work (as opposed to something that is forced upon the staff) then it might be more likely to be embraced by the staff.

We also found that integrating a success item in the scope of staff meetings was often considered viable by the interviewees. However, the overall data gave an impression that currently successes were included either on a superficial level (i.e., they were merely identified without an overt purpose of generating lessons from them or identifying the success factors behind the tasks), or unsystematically (e.g., not explicitly part of meeting agendas). Certain level of steering – if not enforcing – might thus be beneficial in ensuring that the success-related data available in the organization is actually used to its fullest potential. This has implications regarding the *formality* of promoting learning from successes: a formal introduction without due attention on the prevailing culture and practices might put the staff in an awkward situation where the espoused practices might be at odds with the existing ones; and conversely, a too lenient promotion of learning from successes may result in haphazard and unsystematic utilization of the successful experiences.

The contextual nature of the concept of success also brings attention to the importance of *translating* "success" to staff meeting participants in a meaningful way. For instance, a mechanic from reactor maintenance viewed successes as uneventful tasks that have proceeded as described in the work plan (i.e., "normal successes"). In such cases, using the concept of success to prompt discussion may be unfruitful since the path to success is perceived as known and evident (i.e., following the procedures) and nothing special had happened. A more complicated example was provided by a Quality Control (QC) engineer who viewed successes as both the condition where a fault *is* discovered (success of QC) and where a fault *is not* discovered (success of the overall system, assuming that the QC's finding is not false negative). These examples suggest that the mere instruction to consider successes in staff meetings might be too abstract to be usable as such. Rather, it might be preferable to translate the concept of success to the end-users, or creating the means to help the end-users contextualize the concept themselves.

The *choice of forum* for discussing successes also received some attention. In our data, we identified various types of staff meetings that can be distinguished by (at least) the following dimensions (see also Table 9):

- *Primary purpose*: problem-solving meetings (e.g., ad hoc meetings during an event), coordination meetings (e.g., pre-job briefings, project preparation meetings), information collection or sharing meetings (e.g., trainings, educative segments in team or group meetings, post-outage reviews)
- *Frequency*: e.g. daily team meetings in the morning, weekly or monthly group meetings, annual post-outage reviews, one-off modernization project feedback meetings
- *Trigger*: proactive (e.g., planning meetings), reactive (e.g., problem-solving meetings), periodical (e.g., scheduled team and section meetings), continuous (e.g., non-scheduled acquaintances, team work)
- *Formality*: informal (e.g., corridor talks), formal (e.g., pre-job briefings, post-job reviews)
- *Participants*: functional group (e.g., specific team or department), temporary groups (e.g., project meetings), internal (e.g., organization-wide events), external (e.g., industry-wide seminars)

The general observation was that a success item was not found suitable for just any staff meeting. When we enquired from the interviewees whether a particular type of meeting would be suitable for examining successes, we received mixed responses. For instance, an interviewee suggested that successes could be formally brought up in cross-departmental trainings, but not necessarily in weekly or monthly internal team meetings. Then again, another interviewee found that internal group meetings are actually rather good forum for sharing success stories. This discrepancy relates to the formalization issue, and indicates that there is a difference between the formality of the meeting itself, and the formality of discussing successes. It is thus possible that successes are better suited as an informal part in meetings that, regardless of whether they are formal or not, allow informal progression (e.g., internal group meetings), or formally in sessions that are characterized by exclusively formal progression (e.g., cross-departmental trainings).

Table 9. *Examples of staff meetings and their relevance to organizational learning from successes*

Meeting	Purpose	Frequency	Trigger	Formality	Participants	Relevance
Project manager (PM) meets with colleagues to discuss previous tasks	Information collection	One-off	Proactive (to project challenges)	Informal	PM and colleague	Collect best practices to ensure project success
Lifting team gathers together to solve an issue during a lifting task	Problem-solving	One-off	Reactive (to the issue at hand)	Formal	Task team	Innovating to ensure successful recovery
Solutions to failures are discussed in weekly IT group meetings	Information sharing	Weekly	Periodical	Formal	Functional group	Share information about successful recoveries
Operating engineers from the neighbouring units meet casually	Information sharing	Daily	Continuous	Informal	Peer	Share information about good practices across units

Another interviewee noted that lessons learned are rarely shared outside the team because they are too specific; respectively, lessons learned are not received from other groups because they are often specific to them. Therefore, common interests might not be easily found. On the other hand, an example case of successful cross-organizational information transfer was demonstrated by a project manager who was preparing an unprecedented modernization project that involved performing challenging tasks such as transporting and lifting of heavy machinery. In order to ensure the success of these tasks, the project manager utilized his social network within the plant to identify people that had carried out comparable tasks previously and organized informal meetings with them to collect best practices. These findings suggest that one of the factors influencing the use of staff meetings for transferring success-related knowledge is related to the selection of participants. As exemplified by the project manager's case, the nature of the task also plays a role: an extensive and complex task is probably more likely to gain from useful input from others. This underlines the issue of *cross-organizational generalizability* of success-related knowledge, which ultimately may limit the scope of information sharing activities, i.e. if the knowledge is not perceived as useful to another department, there might be no reason to bring the success-related knowledge to a wider forum, and vice versa. Strategies such as abstraction (e.g., the lessons learned would be abstracted by the sender, and then transferred to the receiver, who would then translate the abstract lesson to practice) might be viable workarounds for the issue. However, they are likely to be too laborious and would most likely require motivational support to the parties that pre-process and make the information available. The example of project manager actively collecting information from others illustrates a case where he directly benefits from the information, which provides motivation for any additional effort required to adapt the lessons learned in other contexts.

Finally, some interviewees brought up that the mere sharing of success-related knowledge is not enough for it to be embraced. Rather, it was found that any *initiatives should be well-justified* to others. It was, however, also agreed that there is no fundamental resistance to initiatives – they just need to be properly explained and rationalized. An interviewee described this as a request to explicate what the added value of the initiative is, as opposed to just ordering the change without explanation. This observation highlights the idea that if successes were to be used for the purpose of learning or organizational change, a staff meeting practice of only bringing up the lesson learned from success might not be sufficient and the potentially useful success-related information might be disregarded because it would be perceived as insufficiently justified. Instead, a joint analysis with multiple parties with a focus on how others could benefit from this particular success might be necessary for the success-related information to be actually internalized by those that receive it (cf. joint stakeholder analysis in Skjerve et al., 2017).

3 INTEGRATIVE FRAMEWORK AND DISCUSSION

Since we view successes in relation to expected performance, what is defined a "success" becomes dependent on the perspective of the stakeholders involved. This leads us to utilize a stakeholder-based approach and view staff meetings as potentially serving multiple knowledge management functions depending on what the role of the actor is in relation to the success-related knowledge. For instance, a group meeting can provide a forum for sharing for the individual that possesses success-related knowledge, or a forum for acquisition for another group member.

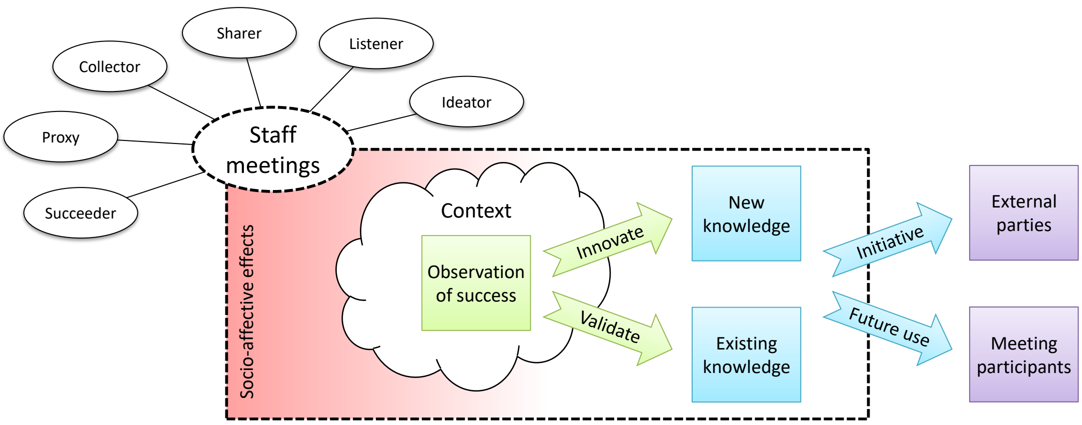


Figure 1. *A stylized illustration of the integrative framework describing the roles and functions of staff meetings*

We propose the following generic functions of success items in staff meeting: a) reinforcement, where successes confirm that the existing knowledge is valid; b) innovation, where the successes provide input for creating new practices and eventually good and best practices through validation; c) socio-affective influences, where successes are utilized for the development of social processes (e.g., culture or team spirit) or for affective responses (e.g., motivation or well-being); d) creating initiatives, where the successes are communicated to external parties; and e) creating knowledge for future use by the meeting participants. These categories serve as the basis for the integrative framework and are illustrated in Figure 1. Based on the findings of our empirical studies, we propose six knowledge management related roles for staff meetings (cf. also Table 9). We view these roles as person-independent, i.e. an individual can assume several roles during a meeting. The list of roles and the potential facilitators and hindrances for the realization of the roles are presented in Table 10, which aims to provide suggestions and ideas regarding how to develop staff meeting practices so as to include a success item.

In this framework, the success item of a staff meeting begins with capturing the observation of success. Depending on the role of meeting participant, this function of the staff meeting can be realized by the roles of Succeeder (optionally facilitated by a Proxy), Sharer, or Collector. The Succeeder is characterized by having the first-hand knowledge of the success. The Succeeder also gains direct motivation from the acknowledgement of the success. However, the Succeeder's role might be affected by the possible cultural influences that inhibit sharing one's own successes. A Proxy can be in an important role in, for example, overcoming the cultural inhibitors to sharing successes, helping staff avoid becoming blind to their successes by questioning or otherwise facilitating the discussion of successes. It is likely that the role of Proxy has some relation to team leadership (either formal or informal), and therefore the Proxy might also have a role in ensuring that right lessons are learned (e.g., avoid complacency and organizational drift) and managing team social dynamics (cf. cultural and social acceptance of sharing successes). The Sharer is in a similar role as Succeeder, but shares someone else's success. By sharing someone else's success, the adverse cultural influences might be overcome. The Collector, unlike Succeeder and Sharer, actively attempts to find other's successes. An individual in such a role can initiate a meeting (or a part of a meeting) for the very purpose of discussing successes another party has achieved. The Collector is also characterized by having a clear learning motivation for the success item, unlike Succeeder and Sharer, who might be motivated by organizational or team-development (e.g., sharing good practices and initiatives) or possibly for receiving praise. Collector, like Succeeder and Sharer, can also relay the knowledge created in one context to another and thus form as a bridge between organizational silos.

Table 10. *Description of the roles, function of staff meetings from the perspective of each role, and potential facilitators and hindrances for the realization of the staff meetings' functions*

Role	Description	Function	Potential facilitators or hindrances
Succeeder	Has first-hand success-related knowledge	Sharing own success experiences	• What cultural influences regarding the acceptability of sharing successes are there? • Are successes understood as meaningful or worthy of mentioning? • Is it natural to share the successes in that particular context?
Sharer	Actively shares success-related knowledge collected from others	Share existing success-related knowledge	
Proxy	Highlights someone else's successes	Share existing success-related knowledge	• Is there blindness towards success-related knowledge (i.e., successes are seen as "business-as-usual")? • Is there reluctance to share successes?
Collector	Actively initiates the collection of success-related knowledge from others	Acquire success-related knowledge from others to serve own goals	• Are those with success-related knowledge known and willing to share their knowledge? • Are there opportunities to initiate the collection of success-related knowledge?
Ideator	Generates new success-related knowledge	Creating new knowledge to solve a problem or to innovate	• Are there methods/tools/capabilities to identify the innovation potential of successes? • Are there methods/tools/capabilities to understand and analyse the success-related knowledge provided by others?
Listener	Receives success-related knowledge from others without actively seeking it	Receive success-related knowledge from others	• What cultural influences are there that affect how receiving the success-related knowledge is perceived? • Is the success-related knowledge perceived as relevant to own work? • How well is the success-related knowledge justified?

The success items in staff meetings can also involve knowledge creation, which is realized by the role of Ideator. For the Ideator, one of the challenges is the initiation of the analysis. Namely, unlike for analysing failures, there are relatively few actual analysis methods with a success focus. Successes – especially if "normal" – are also often hard to grasp analytically in order to create new knowledge.

The Listener is in a relatively passive role in the sense that individuals in this role do not collect, share or create knowledge, but receive the information shared or created by the others, evaluate its usefulness and then utilize it in their own work afterwards. For this role, it is important to get sufficient justification from the sharers or creators for the information to be truly internalized. The information also needs to be both actually relevant, but also perceived as relevant. This means that the sharers or creators of the information need to understand the needs of the Listener.

One of the main insights of the framework comes from the stakeholder approach, which aims to uncover *what the meaning and the perceived value of success-related information is to each actor* that is reached by the tool. This directs attention to topics such as: a) the translation of the concept of success to context (e.g., explaining what types of successes there are and how they relate to a given actor's task); b) the identification of those to whom the success-related knowledge can be beneficial and thus should be shared to (e.g., creating generalizations and links within and outside the particular staff meeting); c) the justification of the success-approach and the relevance of lessons learned from successes to others; and d) the identification of those who possess relevant information. The stakeholder approach also reveals that there can be interrelations between the roles (e.g., the role of Proxy in overcoming cultural bottlenecks of sharing success-related knowledge).

Another important insight from the framework is that success items in *staff meetings can serve multiple functions* (i.e., reinforcing existing knowledge, creating new knowledge, or inducing socio-affective effects), and that the interrelation of these functions can have adverse consequences to safety if not properly managed. For example, if a successful outcome has been achieved by means of cutting corners or other bad habits, acknowledging the success will reinforce these practices. Thus, especially when using past successes for inducing positive socio-affective effects (e.g., improving motivation or building team spirit), one should at the same time ensure that the processes that led to a successful outcome are properly understood, i.e. that not only the outcome was successful, but also the way in which it was achieved.

4 CONCLUSIONS

In this paper, we have described the results of a modelling exercise with the purpose of shedding light on how a concrete knowledge management method – staff meetings - can facilitate organizational learning from successes. We propose that the resulting integrative framework and the principles utilized in this exercise could be, with some modifications, also usable for modelling other methods (e.g., formal reporting systems or internal communication practices). The modelling exercise can be a potentially useful tool for safety practitioners, supervisors and other experts in safety-critical organisations aspiring to implement activities that facilitate learning from successes. The insights presented in the framework can also be useful in ensuring that the potential positive effects of success items are achieved and the potential negative ones are avoided. Balancing this trade-off is also important in ensuring that striving towards the approaches suggested by modern safety management approaches such as Resilience Engineering and Safety-II result in improved safety.

Acknowledgements

The work presented in this paper is based on a research project funded by SAFIR2018, Vattenfall AB and NKS. The authors are grateful to the power companies for their cooperation and support during the case studies.

REFERENCES

De Long, D. W., & Fahey, L. (2000). Diagnosing cultural barriers to knowledge management. The Academy of Management Executive, 14(4), 113–127.

Garvin, D. A. (1993). Building a learning organization. Harvard Business Review, 71(4), 78–91.

Hollnagel, E. (2014). Safety-I and safety–II: the past and future of safety management. Farnham, Surrey: Ashgate Publishing, Ltd.

Hollnagel, E., Pariès, J., Woods, D. D., & Wreathall, M. J. (2011). Resilience Engineering in Practice: A Guidebook. Great Britain: Ashgate Publishing, Ltd.

IAEA. (2008). Best practices in identifying, reporting and screening operating experience at nuclear power plants. Vienna: International Atomic Energy Agency.

Madsen, P. M., & Desai, V. (2010). Failing to learn? The effects of failure and success on organizational learning in the global orbital launch vehicle industry. Academy of Management Journal, 53(3), 451–476.

Skjerve, A. B., Viitanen, K., Axelsson, C., Bisio, R., Koskinen, H., & Liinasuo, M. (2017). Learning from Successes in Nuclear Operations – A Guideline. Presented at the ESREL2017, Portorož, Slovenia.

Viitanen, K., Bisio, R., Axelsson, C., Koskinen, H., Liinasuo, M., & Skjerve, A. B. (2016). Learning from Successes in Nuclear Power Plant Operation - Intermediate Report from the NKS-R LESUN (No. NKS-354). NKS.

BUILDING AN "ADAPTIVE SAFETY CULTURE" IN A NUCLEAR CONSTRUCTION PROJECT – INSIGHTS TO SAFETY PRACTITIONERS

Kaupo Viitanen [1] and Teemu Reiman [2]

[1] VTT Technical Research Centre of Finland LTD, P.O. Box 1000, FI-02044 VTT, Finland

[1] kaupo.viitanen@vtt.fi

[2] Consultant

Abstract

Nuclear power plant construction projects are challenging for safety management due to many of their inherent characteristics, which include high levels of organizational turbulence, changes in lifecycle phases, unanticipated events, interactions between multiple parties and the challenges of multicultural environment. This means that traditional approaches to improving safety might not be sufficient. To address this issue, we will view safety management from the perspective of Resilience Engineering and complexity thinking and propose a novel perspective to the practical development of safety culture in dynamic environments. We describe a revised model of adaptive safety management and use four well-known safety culture improvement methods as illustrative examples of how they can be utilized in building an adaptive safety culture.

1 INTRODUCTION

Managing safety in turbulent environments creates extra challenges for the creation of a strong safety culture. For example, in nuclear power plant (NPP) construction projects, some of the common challenges include growth of personnel at the participating companies, changes in the phase of the project as the project proceeds, various unanticipated occurrences, multiple interacting parties and multicultural environment. This implies that traditional approaches to safety assurance which have been developed for more stable organizations might not be sufficient anymore.

A novel approach to organizational management is the application of complexity theories. This approach postulates, for example, phenomena such as change through self-organization, emergent patterns that cannot be traced back to individual elements, non-linear relation between inputs and outputs and irreversibility (Reiman, Rollenhagen, Pietikäinen, & Heikkilä, 2015), and emphasizes the importance of understanding and managing trade-offs or tensions. The latter has been widely recognized in the field of organizational studies (e.g. Cameron & Quinn, 2006) and safety science (e.g. Amalberti, 2013; Woods & Branlat, 2011). We propose that an NPP construction project can be viewed as a complex sociotechnical system, involving a variety of tensions and paradoxes that can manifest themselves, for example, as conflicting organizational requirements or goals. Overall, this suggests that safety management should be based on the key features of how complex systems function, and make use of those features, not only seek to dampen them (Carrillo, 2011; Reiman et al., 2015).

Basing on the characteristics of complex adaptive organizations and existing models, Reiman et al. (2015) have proposed an *adaptive model of safety management* which identifies four tensions, each consisting of a conflicting pair of management goals: 1) *system goals – local goals* 2) *repeatability and systematic response - flexibility and adaptability,* 3) *low system variance – high system variance*, and 4) *few strong ties – multiple weak ties*. The model was used by Reiman (2015) to highlight the different roles that safety practitioners need to take in an organization, depending on factors such as organizational core task and culture, current level of safety, and external factors such as changes in legislative requirements or societal values. A weakness of the model is that it combines several different types of issues into one model, such as the goals of safety management in complex adaptive systems (*why, what*) and the working practices to reach those goals (*how*). The model also lacks guidance for selecting the concrete methods to facilitate and monitor the fulfilment of the principles (*what, how, when*). Finally, the model should offer holistic view of the various activities taking place in the organization, and their direct and indirect effects in order to avoid decomposition and reduction of the complex adaptive system into seemingly independent factors – with their linear causal effects.

In this paper we will describe the essential characteristics of "adaptive culture", present a revised model of adaptive safety management and discuss how the model can be applied in the context of safety culture improvement. We will focus on the following well-known approaches to safety culture management: *monitoring* of the state of safety culture in the organization, bottom-up and top-down *safety-related communication*, and *direct behaviour modification*. A concrete safety culture improvement tool from each category is selected and examined from the perspective of the revised model of adaptive safety management. This exercise is intended to shed light on how conflicting safety management principles can manifest themselves in the concrete activities of safety practitioners, and highlight the paradoxical nature of these programmatic methods of changing complex sociotechnical systems. We propose that the utilization of this model in the practical implementation of safety culture improvement methods can help safety practitioners (especially middle-level) in high-risk organizations use these methods effectively and successfully.

2 ADAPTIVE SAFETY CULTURE

Resilience Engineering research tradition emphasizes that system safety is an emergent property of the system and should be seen as the system's ability to succeed under varying conditions (Hollnagel, 2011). Thus, system safety requires adaptive capacity. We argue that this adaptive capacity should be supported by what we call an *adaptive culture*. By adaptive culture we refer to an organizational (safety) culture that allows and supports qualitatively different – even contradicting – organizational manifestations of safety management (e.g. structures, tools, practices), depending on the anticipated and actualized needs of the organization. Adaptive safety culture embeds the assumptions that view safety systemically and as requiring a diverse means for managing it. The assumptions of an adaptive safety culture are not constraining even though its actions can sometimes be. An adaptive safety culture does not assume a command and control strategy as the preferred, or the only, way of managing safety, but it is still able to utilize those strategies when needed. An adaptive safety culture also needs to have the means to monitor itself and its adaptations (Hollnagel, 2011; Reiman et al., 2015; Reiman, Rollenhagen, & Viitanen, 2014). In summary, an adaptive safety culture should create the organizational preconditions to cope with anticipated and unexpected situations, and acknowledge the inherent adaptive nature of sociotechnical systems.

Adaptive safety culture becomes especially important in situations of external or internal change. For example, in an NPP construction project, a change in the lifecycle phase from design to construction, or construction to commissioning, requires both new types of activities, and changes to the existing activities. The same applies if there are changes in the project participants' safety culture. For instance, in early phases of the project, different methods are likely to be needed when the participants do not know each other, are not familiar with the specific requirements of the project, or do not have the necessary organizational preconditions in place. Once these have been established, the development of safety culture can proceed to utilize other types of methods and approaches. Alternatively, the methods can remain the same but they have different effect because the system has changed.

3 ADAPTIVE SAFETY CULTURE MANAGEMENT

3.1 Revised model of adaptive safety management

In the revised model of adaptive management we included three tensions and a three-phase continuous improvement cycle (Figure 8). The selection of tensions is based on the assumptions that a complex sociotechnical system is multilevelled (i.e. involves upper and lower systemic levels), has the ability (and tendency) to self-organize, and involves interactions between multiple agents (e.g. Reiman et al., 2015). The first tension, levels of system goals, addresses the questions "*why*" and "*what*", and stems from the multilevelled nature of the system. This tension also involves the idea of temporality, namely that system goals are typically longer-term, and local goals are shorter-term. The second and third tensions represent safety management strategies, i.e. address the question "*how*". Each tension is characterized by contradicting safety management principles (the boxes in Figure 8). The model also embodies the idea that in order for the safety management to be functional in a sustainable manner, it must have the capability to utilize all of the principles, regardless of whether they are at odds with each other. This means that the tools (and the way in which they are) utilized by the safety practitioner should be sufficiently diverse in order to cover the whole spectrum of the model.

Including the three-phase continuous improvement cycle addresses the shortcomings of the previous model (chapter 1) and aims to answer the questions "*what*", "*how*" and "*when*". The cycle thus represents the kinds of actions that a safety practitioner can (and should) utilize for improving safety culture; furthermore, all three tensions influence (and are influenced by) the activities conducted in each of the phases. The continuous improvement cycle draws from concepts such as the Plan-Do-Check-Act cycle and the temporal elements of Resilience Engineering cornerstones (Anticipate, Monitor, Respond) and includes the following phases (with descriptions of their meaning in the context of safety culture improvement):

- *Do and correct*: implement safety culture improving structures or influence behaviour of organizational members; correct or adjust those activities that have been found detrimental or ineffective for safety culture improvement
- *Monitor*: assess the basic assumptions regarding safety and their manifestations, including the way in

which adaptations are made, what organizational structures are implemented and how they are utilized

- *Review and plan*: analyse the strengths and weaknesses from the results of past safety culture monitoring and implementation activities, anticipate future challenges and opportunities, and devise plans for future safety culture monitoring and implementation activities

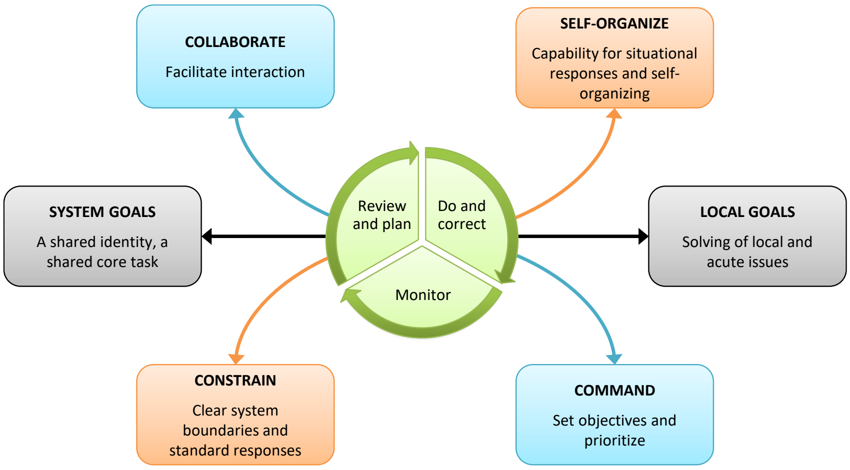


Figure 8. *Revised model of adaptive safety management. The grey boxes depict the levels of system goals, teal and orange boxes depict the safety management strategies to achieve the goals. The arrows indicate the tensions between the system goals or strategies. The continuous improvement cycle in the middle depicts the kinds of concrete safety culture improvement actions taken by safety practitioners*

3.2 Safety culture improvement tools

Audits (monitoring)

The use of auditing is a popular method for evaluating the extent to which a set of defined requirements is met. Audits are commonly used in the evaluation of management systems – either for internal development (i.e. internal audits), subcontractor evaluation (i.e. second-party audits) or for certification purposes (i.e. third-party audits). The requirements are defined, depending on audit type, either by internal company targets or by various standards such as the ISO9001 standard for quality management systems. To date, nuclear safety culture has rarely been evaluated by means of auditing. Audits as a safety culture evaluation method have been criticized as having excessive focus on structures and processes and not enough on how these structures and processes are applied in practice (e.g. Reiman, Pietikäinen, & Oedewald, 2008). However, there are cases where safety culture has been included in the audit agendas of safety management audits or quality standards. For example, the ISO9001-derived, nuclear-specific quality standard NSQ-100 includes requirements and guidelines for safety culture. Recently, audits have also been applied for evaluating safety culture in the nuclear industry supply chain (Reiman, Viitanen, & Koivula, 2017).

Reporting of near-misses and safety concerns (bottom-up safety-related communication)

Organizations aiming at a high level of safety strongly encourage personnel to report errors and near misses. Various types of reporting systems can by utilized for collecting information from the employees. The systems can be voluntary or mandatory, confidential or non-confidential. In this paper we focus on reporting systems that are voluntary and where personnel can make reports either with their own name or anonymously if they wish. Management uses the feedback received via the reporting systems to identify organizational problems and help individuals and teams learn from mistakes in order to perform better in the future. Documenting and learning from patterns of failure provide free lessons for organizations that are successful in acquiring this kind of feedback (DoE, 2009, p. 95).

Safety training (top-down safety-related communication)

Safety training is likely to be the most commonly used practical method that has an explicitly stated focus of safety culture improvement. Safety trainings come in many forms and can range from short talks that are embedded within induction trainings or pre-job briefings, to extensive multi-week seminars and lecture courses on technical, human or organizational topics. Safety trainings serve many purposes depending on their content and focus. For instance, they can develop safety culture related awareness, behaviour or attitudes (e.g. Harvey, Bolam, Gregory, & Erdos, 2001; IAEA, 2002), and can be targeted at any level of the organization, including shop-floor, supervisors and middle management, and top management.

Human Performance Programs (direct behavioural modification)

The goal of a Human Performance Program (HPP) is to introduce and formalize a set of "good working practices", a.k.a. Human Performance Tools (HPTs), which are to be used by the members of the organization, typically shop-floor personnel (DoE, 2009; Oedewald, Skjerve, Axelsson, Viitanen, & Bisio, 2015). The HPTs are very heterogeneous and include practices such as Pre-Job Briefing (a meeting held before performing a given task), Post-Job Review (a meeting held once a given task is completed), Self-Checking (e.g. stopping to think and reflect before carrying out a task) and Clear Communication techniques (e.g. the use of three-way communication or phonetic alphabets) (see further descriptions in DoE, 2009). Usually the proclaimed objective of HPTs is to standardize working practices in order to avoid human error.

3.3 Safety culture improvement tools in light of the revised model

The safety culture improvement tools described in previous chapter are the concrete manifestations of the continuous improvement cycle. The segment "*do and correct*" includes, for example, the implementation or revision of an auditing process or a reporting system, conducting safety trainings, introducing a HPP, or using HPTs. Respectively, the segment "*monitor*" involves the use of auditing or reporting systems for information collection, gathering feedback from safety trainings (e.g. participant comments, test results) or from employees using HPTs. This means that the same tools can belong to both segments, but the "*do and correct*" phase is about implementing the tool and using it, while "*monitor*" phase is about receiving information about the organization or the tool's functionality. The segment "*review and plan*" integrates the information received from "*monitor*" or anticipates future requirements to produce a revision or a new plan for safety culture improvement, including the selection of tools and the way in which they are to be implemented.

The safety practitioner can utilize safety culture improvement tools to develop an adaptive culture by ensuring that the tools being used contribute to all of the principles of the model of adaptive safety management. An overview of the primary and secondary influences of the safety culture improvement tools, along with some insights regarding the factors to be considered when utilizing the tools, is presented in Table 11.

One of the main insights of this exercise is that *not all tools contribute to all principles* and that *some tools can contribute positively to one principle, but negatively to another*. For instance, audits, by definition, attempt to identify the non-conformities and deviations from requirements, thus focusing strongly on decreasing the self-organization and variability within the system (i.e. primary focus on "*constrain*"). On the other hand, due to the uniqueness of the characteristics of the operational environment of each auditee, certain level of local diversity (i.e. capability for "*self-organization*") may need to be retained. Thus, safety culture improvement through auditing may result in undesirable outcomes such as limiting the auditee's capability to cope with its inherent environment. Respectively, in the case of safety trainings, that can be utilized to disseminate and acculturate employees to company-wide practices or values, the focus is on ensuring that everyone contributes to achieving a common goal (i.e. contributes to "*system goals*"). Additionally, through the development of knowledge and skills, safety training can also result in the formation of, for example, a better understanding of the role of own tasks in relation to safety, the effects of humans and organizations on safety, and a wider understanding of the hazards that relate to the various organizational tasks (i.e. contributes to "*self-organize*").

A given tool can also contribute positively or negatively to a given principle, depending on how the tool is implemented. For example, at first glance HPTs may appear to focus on promoting repeatability and standard responses, and thus on limiting self-organization and system variance (i.e. "*constrain*"). However, in practice HPTs can also to contribute to safety by enabling knowledge sharing, improving the understanding of the work environment and sensitizing to the unexpected (Viitanen, Axelsson, Bisio, Oedewald, & Skjerve, 2015), and creating a shared culture (Viitanen & Oedewald, 2015). This means that HPTs can also be seen, for example, to promote a shared identity and understanding of system goals, to create the capability for adaptation and to facilitate the interconnections between various organizational members (i.e. "*self-organize*", "*system goals*" and "*collaborate*"). The implementation strategy is one of the key elements that determine how the introduction of a HPP will end up affecting the system (Viitanen et al., 2015). For example, the communication of the content of the HPTs and the intention of their use, and their collaborative design together with the end-users have been identified as essential steps for the successful implementation of a HPP (Oedewald et al., 2015) (emphasizing the need for the principles of "*collaboration*" and "*self-organize*"). On the other hand, if too much lenience and decentralization is allowed in the implementation process, the benefit of HPTs as shared good practices might be reduced, which means that the safety practitioner needs to take the other end of these tensions (i.e. "*constrain*" and "*command*") into account during the implementation as well. This might involve, for example, sanctioning and enforcing the use of certain HPTs in certain situations.

A related insight is that the *tool may require the fulfilment of certain preconditions to be functional, or to function as intended*. For example, for a voluntary reporting system to function in practice, certain organizational characteristics are required. One of these preconditions is the creation of "just culture" (Reason, 1997), which involves the management getting the balance right between how unintentional errors and wilful violations are addressed in the organization (i.e. ensuring specific type of "*system goals*").

Table 11. *The influences of safety culture improvement tools on management safety principles*

Tool	Primary influences	Secondary / potential influences	Things to consider
Audits	Auditing contributes to **constrain** by verifying compliance against predefined standards or requirements	Auditing of safety culture can also be used to steer (**command**) the auditee to focus on the issues of interest to the auditor Auditing can also be used to facilitate **system goals** by focusing on issues that are relevant based on the project's overall needs	Due to sample-based approach, auditing can contribute negatively to **local goals**, because it can lead the auditee to only focus on the issues identified in the audit The focus on **constrain** can hide the requirements of **self-organize**, and focus too much on structure instead of actual organizational potential
Reporting systems	Reporting systems contribute to **local goals** by encouraging and making it possible for the personnel to report near-misses and concerns they have about their own work	Reporting systems can also contribute to **self-organize** by pointing out issues in daily work that can be improved **System goals** can be facilitated by reporting depending on personnel's capacity to see the wider implications of daily problems	Reporting systems are dependent on **collaborate**. If there is a lack of trust and collaboration, they are likely to not function properly. A focus on **system goals** is required to establish a culture of trust and fairness The reporting systems may also further deteriorate **collaborate** if the personnel begins reporting minor issues that could easily be solved by communication and collaboration
Safety training	Safety trainings contribute to **system goals** by highlighting the importance of safety as a shared value and facilitating its formation through acculturation	Safety trainings can also contribute to **self-organize** by increasing knowledge and skills and widening the understanding of what safety means in a construction project	Using training as a safety culture improvement method can easily be interpreted by personnel as a **command** strategy if it is perceived as too one-sided
Human performance tools	HPTs contribute to **constrain** by promoting standard practices such as checking and verification practices, communication procedures, etc.	HTPs can also contribute to **self-organize**, e.g. by promoting STAR principle (Stop, Think, Act, Review) as a standard response or by facilitating learning through Post-Job Reviews	HPTs require some **command** to be fully implemented, yet their internalization and acceptance by the personnel requires **collaborate**. A heavy focus on only one of these two strategies will help in implementing the tools but may ultimately reduce the effectiveness of the tools

4 CONCLUSIONS

In this paper we have introduced the concept of adaptive safety culture, discussed its relevance in the context of NPP construction projects, proposed a revised model of adaptive safety management which explicates the safety management principles relevant to complex sociotechnical systems, and conducted an exercise that examines how practical safety culture improvement tools commonly available to any safety professional are related to the revised model of adaptive safety management. The revised model can offer several insights to safety practitioners aiming to improve the safety culture. These include:

- Highlighting the contributions that a given safety culture improvement tool has to the principles of

adaptive safety management
- Helping identify the weaknesses of the safety culture improvement tools in relation to the other safety management principles
- Highlighting the fact that all safety culture improvement tools embed certain principles yet these principles are interpreted by the safety professionals resulting in variability in the use of the tools in practice

In contemporary safety-critical organizations characterized by uncertainty and turbulence, utilizing an adaptive approach to safety management is especially relevant. By utilizing the revised model of adaptive safety management, safety practitioners can better plan, implement, monitor and review the activities conducted to improve safety culture in order to ensure that an adaptive safety culture is formed – one that embraces self-organization and collaboration, but also understands their limitations and is capable of utilizing the opposite strategies of command and control when needed.

REFERENCES

Amalberti, R. (2013). Navigating Safety. Dordrecht: Springer Netherlands.

Cameron, K. S., & Quinn, R. E. (2006). *Diagnosing and changing organizational culture: based on the competing values framework* (Rev. ed). San Francisco: Jossey-Bass.

Carrillo, R. A. (2011). Complexity and safety. Journal of Safety Research, 42(4), 293–300.

DoE. (2009). *Human Performance Improvement Handbook Volume 2, Human Performance Tools for Individuals, Work Teams, and Management*. Department of Energy Washington, DC: Government Printing Office.

Harvey, J., Bolam, H., Gregory, D., & Erdos, G. (2001). The effectiveness of training to change safety culture and attitudes within a highly regulated environment. *Personnel Review*, *30*(6), 615–636.

Hollnagel, E. (2011). Prologue: the scope of resilience engineering. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice: A guidebook* (pp. xxix–xxxix). Great Britain: Ashgate Publishing, Ltd.

IAEA. (2002). *Safety culture in nuclear installations: guidance for use in the enhancement of safety culture*. Vienna: International Atomic Energy Agency.

Oedewald, P., Skjerve, A. B., Axelsson, C., Viitanen, K., & Bisio, R. (2015). *Human performance tools in nuclear power plant maintenance activities - Final report of HUMAX project* (No. NKS-328). NKS.

Reason, J. (1997). *Managing the Risks of Organizational Accidents* (1 edition). Aldershot, Hants, England; Brookfield, Vt., USA: Ashgate.

Reiman, T. (2015). *Turvallisuusasiantuntijoiden roolit, toimintatavat ja tarvittavat kyvyt ja taidot* (VTT Technology). Espoo: VTT Technical Research Centre of Finland.

Reiman, T., Pietikäinen, E., & Oedewald, P. (2008). *Turvallisuuskulttuuri: teoria ja arviointi*. Espoo, Finland: VTT Technical Research Centre of Finland.

Reiman, T., Rollenhagen, C., Pietikäinen, E., & Heikkilä, J. (2015). Principles of adaptive management in complex safety–critical organizations. Safety Science, 71, Part B, 80–92.

Reiman, T., Rollenhagen, C., & Viitanen, K. (2014). On the relation between culture, safety culture and safety management. In *12th International Probabilistic Safety Assessment and Management Conference, PSAM 2014, 22 June 2014 through 27 June 2014*.

Reiman, T., Viitanen, K., & Koivula, N. (2017). Safety Culture Assurance by Auditing - limits and possibilities. Presented at the 9th International Conference on the Prevention of Accidents at Work, Prague, Czech Republic.

Viitanen, K., Axelsson, C., Bisio, R., Oedewald, P., & Skjerve, A. B. (2015). Enhancing Resilience by Introducing a Human Performance Program. Presented at the 6th REA Symposium, Lisbon, Portugal.

Viitanen, K., & Oedewald, P. (2015). Human performance programmes as a means to improve safety culture. In P. Oedewald, N. Gotcheva, K. Viitanen, & M. Wahlström (Eds.), *Safety culture and organisational resilience in the nuclear industry throughout the different lifecycle phases* (pp. 52–66).

Woods, D. D., & Branlat, M. (2011). Basic patterns in how adaptive systems fail. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), *Resilience Engineering in Practice: A Guidebook* (pp. 127–144). Great Britain: Ashgate Publishing, Ltd.

RESILIENT POWER PLANT OPERATIONS THROUGH A SELF-EVALUATION METHOD

Mikael Wahlström[1], Timo Kuula[1], Laura Seppänen[2], Piia Rantanummi[3], Pekka Kettunen[3]

[1] VTT Technical Research Centre of Finland Ltd, Vuorimiehentie 5, FI-02150, Espoo, Finland

[1] mikael.wahlstrom@vtt.fi; timo.kuula@vtt.fi

[2] Finnish Institute of Occupational Health FIOH, Arinatie 3 A, FI-00391, Helsinki, Finland

[2] laura.seppanen@ttl.fi

[3] Fortum Power and Heat Oy, Loviisa Nuclear Power Plant, Atomitie 700, FI-07901, Loviisa, Finland

[3] piia.rantanummi@fortum.com; pekka.kettunen@fortum.com

www.vtt.fi; www.fioh.fi; www.fortum.com

Abstract

Well trained operators are essential for safety. This study presents a self-evaluation method to be applied after simulator training by power plant operators. The method was created collaboratively with training developers at a nuclear power plant. Inspiration was drawn from education theory as well as from resilience engineering literature. In particular, we considered the line of study that suggest that 'interpretive practices' (which involve, e.g., robust communication and the use of various information sources critically) support system resilience. Drawing from this line of study, the developed training method encourages operators to reflect on their own work practices. In practice, the method consists of individual self-evaluation and group discussions. The method was tested with four operator shifts. A brief analysis on the group discussions is presented. It suggest that applying the method might be beneficial for system resilience because a significant proportion of the discussions supported reflection concerning issues that may support system resilience: collaboration, understanding of plant dynamics and the use of procedures. We assume that this kind of 'developmental reflection' could potentially enhance work practices. Overall, we suggest that developmental reflection may open avenues for supporting the learning dimension of interpretive practice and thus also resilience.

1 INTRODUCTION

Capability for responding on emergencies and incidents depend on the work practices of the operators handling the situation in question. In other words, the quality of work practices promotes system resilience. Reflecting this line of reasoning, differences in how nuclear power plant operators handle emergencies in simulator training has been studied: some operator teams expressed more 'interpretive' work practices than others, that is, their work practices involved features such as application of various information sources, double-checking of information, anticipation of situations and appropriate dialogue (Savioja, Norros, Salo, & Aaltonen, 2014). As it is assumed that these interpretive practices promote system resilience, one may also assume that developing training for more interpretive performance could enhance system resilience.

For enhancing simulator training in the nuclear domain, we have generated a self-evaluation method that aims to disseminate and create good work practices by the means of guided dialogue among the operators. It consists of 1) personal evaluation, 2) group evaluation and 3) inter-group discussion (the last phase is still to be actualized). Two questionnaires were constructed for self-evaluations of the first two phases, including simulator task performance related open-ended questions and statements with rating scales. A brief analysis of the use of the method is presented.

2 THE STUDY CONTEXT

2.1 Nuclear power plant operations at the studied site

Our study concerns a European nuclear power plant site. The plants at the site apply pressurised water reactors, which is a common reactor type. The operator teams for these plants consist of three assignments: 1) shift supervisor (whose responsibility is the plant's overall operating activity and has the final word in decision-making), 2) reactor operator (who controls the primary circuit, that is, the heat and pressure transfer, as produced by fission, at the shielded core of the plant), and 3) turbine operator (who controls the secondary-circuit, that is, the heat and pressure transfer rotating a turbine connected to a generator that produces electricity). The work takes place day and night. The operators monitor the plant process for achieving safety in all possible situations.

The operators have an engineering degree and in addition to this they have acquired training at the plant in the beginning of their career. This training involves fifteen work-weeks at the simulator, in addition to class-room training, written exams, co-working with the experienced operators and visits at different parts of the plant.

After the initial training, the operators are required to study throughout their career. This consists of simulator training, classroom lessons and self-study. New operating procedures, which have to be learnt, are introduced occasionally and the operators have to pass exams for renewing their operating license. Simulator training is mandatory, as required by the authorities.

The simulator meticulously replicates the control room layout as well as the plant dynamics. The controls consist of desks and three walls filled with analogue controls. The fourth wall includes paper files filled with operating procedures and few analogue controls. The control layout corresponds with the plant dynamics: the causal links and devices of the plant (steam lines, pumps, generators and such) are replicated on the control walls. Some newer digital tools have been introduced to the control room, these including computers for monitoring the plant dynamics and there is also a newly fitted digital control device for a specific function at the plant – but this too is linked to the analogue relays of the plant. The shift supervisor monitors the plant at the centre of the large room while the reactor operator and the turbine operator are situated to the front-left and front-right of him/her, respectively.

2.2 Resilience in NPP operations – the interpretive practice approach

In the case of an emergency, alarms and procedures are important in the operation of the plant. The procedures, which are printed on paper, include flow-charts to be followed and all of the three operator types have their own procedures. Furthermore, during emergencies (and sometimes during emergency training) a supplementary safety engineer will join the operator team; s/he monitors the plant state, based mainly on measures, and has her/his own set of procedures. The plan is then that control actions are dictated by the procedures during critical situations and that there would be procedures to all hazardous situations (in regular conditions the usage of the plant is less proceduralised). However, in view of the resilience engineering thinking (Hollnagel, Woods, & Leveson, 2007) individuals' problem solving capabilities are essential because no system can be designed to be completely safe.

As mentioned earlier, operator shifts seem to apply procedures in differing manners. As work practices were compared, some shifts were found to be more interpretive than others: parameter-based anticipation, critical consideration of multiple sources of information, discussion and double-checking activity were identified in varying prevalence (Savioja et al., 2014). One may assume that with dialogical interpretation of the situation, better problem solving can be achieved. In other words, the existence of 'interpretive practice' promotes system resilience (Norros, Savioja, & Koskinen, 2015). Furthermore, in involving dialogue and interpretation, one may assume that interpretive practice promotes learning, that is, it supports continuous learning.

2.3 Training challenges at NPP sites

As found by Wahlström and Kuula (2016) there could be certain shortcoming and challenges in organising new learning in the NPP domain. Firstly, based on studying a particular NPP site, there seems to be lack of exchange in good work practices. In particular, there were not possibilities to witness the work practices of colleagues in one's own work role (for instance, shift leaders could not see other shift leaders' work practices). Secondly, there were limited resources for training in one's own terms and according to shift or operator specific needs. The content of class-room training days was largely (though not fully) dictated top-down. Furthermore, the current safety procedures dictate operator activity very specifically – understanding of the plant dynamics for enhancing the capability to handle new kinds of situations is therefore not very efficiently developed in the emergency training where these procedures are applied, which is problematic for developing resilience.

Although these notions are based on studying a specific power plant site, it is possible that they are customary in the NPP domain: the NPP operating organizations are typically quite old and large, given that huge resources are needed and that the nuclear technology has been in widespread civilian use for more than half a decade. This could imply inflexibility in adopting new learning methods efficiently. The stringent regulations of the NPP domain have been found to influence design processes: there is present the need to balance between creating new solutions and fulfilling requirements (Gotcheva, Oedewald, Wahlström, & Macchi, 2016; Macchi et al., 2014; Macchi et al., 2013); a dilemma of this kind could be present in training development as well.

3 THE SELF-EVALUATION METHOD

3.1 Education theory

Our study for improving training is informed by cultural-historical approaches to psychology and activity. More specifically, we were inspired by the Finnish Change Laboratory tradition (Virkkunen & Newnham, 2013) and the French Activity Clinic approach (Clot, 2009; Seppänen et. al., 2016). The change laboratory involves identifying the challenges the current training practices, along with the explicative historical reasons to these, as well as solutions. Change laboratory is a collaborative method: new concept for training can be identified and generated together with the workers. The Activity Clinic approach entails that the workers would better consider their own work performance, alone and together with others. In line with these thoughts, the method proposed was developed in close collaboration with the studied nuclear power plant operating organization and it aimed promoting operators' occupational self-reflection (individually and in groups).

Informed by the approaches named above, we paid attention to the developmental effects of the self-evaluation method. We assume that the developmental dimension of 'interpretive practice' (which is discussed above) could be enhanced by training. Overall, however, the method applied in this study is more steered by the practical circumstances and preconditions of training rather than any given education theory or method.

3.2 Creating the self-evaluation method

The identified challenges and discussions with the NPP workers (see 'Training challenges in NPP domain. above) (Wahlström & Kuula, 2016) provided the basis for development of the self-evaluation method. In particular, the aim was to develop a method that would help in proliferation and creation of good work practices bottom-up, that is, as initiated by the operators themselves. It was decided that the method should be connected to the simulator-training, since it is in this environment especially where the operators apply their know-how for resolving difficult situations.

In collaborative development of the method, which involved work-shops between the researchers and training developers at the NPP site, practical limitations as well as the existing knowledge-base of the organization were considered. On limitations, we concluded that the method would have to be applicable by the operating organization even without the researcher involvement and therefore the process of applying the method could not be very time-consuming – it would be unrealistic to attain time-recourses for this at least in the very beginning of the method implementation.

On the existing knowledge-base, in turn, we considered the existing criteria for good work in particular. The evaluation criteria applied by the trainers at the operating organization for evaluating simulator performance were considered applicable for self-evaluation as well – they involved the basic elements involved in operating the plant, these being: 1) process supervision, 2) process control & plant dynamics, 3) safety thinking, 4) use of procedures and 5) communication and co-operation. In addition to these criteria provided by the plant, we also considered the issue of 6) stress management here (since it also something that is to be considered in emergencies and is also present in simulator training (Pakarinen, Korpela, Torniainen, Laarni, & Karvonen, 2016)) and 7) new learning (during the simulator training). All these issues involve elements that could support interpretive practice.

3.3 The self-evaluation method process

The post-simulator self-evaluation method involves three phases, which are to be actualized after simulator training sessions. The first two phases, these being 'individual self-evaluation' and 'group self-evaluation', were actualized almost directly after the simulator sessions (a small recreational pause was taken) while the third phase 'dissemination of good work practices between shifts' is to be actualized on a separate day (during writing, this is still to take place, but it will involve collecting the responses from individual and group self-evaluation and reviewing them among the shifts). Four different shifts applied the method after a simulator training session (which involved four simulator exercises). The operators wrote down their responses in individual and group self-evaluation. The group self-evaluation discussions were recorded for analysis.

Individual self-evaluation

Fifteen minutes were given to the actualization of the individual self-evaluation. The aim of these questions was to encourage the operators to think about their own exercise and what was learnt. Further, the element of stress was involved for facilitating discussion on this subject in the group evaluation phase (i.e., the Likert scale response was not of interest in itself). The self-evaluation instruction (which were printed on a paper and the response was given hand-written) involved the following items:

1. Open questions:
    a. What were the learning aims of the exercise?
    b. Was there a particularly successful phase or event in the exercise? What was that (describe)?
    c. What was the most difficult phase or event in the exercise? How did you handle the challenging situation (how did you react, what did you do, etc.)?
    d. In hindsight, what would you do differently?
    e. Did you learn something new? What was that?
2. Self-evaluation on a 1–5 Likert scale by criteria applied by the operating organization; the elements of the assessment tool are as follows (the items cannot be fully enclosed here):
    a. Process supervision (maintenance of situation awareness and understanding of the overall plant state)
    b. Process control & knowledge of plant dynamics (prediction of plant state vis-á-vis control procedures and acquisition of knowledge)
    c. Safety thinking (safety as aim in all situations and work practices for supporting safety)
    d. Use of procedures (adherence to and use of procedures in all situations, communication about the procedures with others and following of plant state in addition to the procedures and reacting to that if needed)
    e. Communication & co-operation (construction of understanding of the system state with others, communication of one's own process control activities, communication outside the control room)
3. Self-evaluation on a 1–5 Likert scale (ranging from 1 'not at all' to 5 'very much') regarding stress:
    a. How stressed were you during the exercise?
    b. How much did stress interfere with your performance?

Group self-evaluation

Thirty minutes were given to the actualization of the group self-evaluation. In the group self-evaluation, each shift first reviewed the power plant's established criteria of 'very good' performance (see the items 2a–2e of individual self-evaluation) as written on paper (i.e., five items in total). After this, the instructions entailed the following open items for the purpose of guiding the discussion on the exercise and for developing activities:

4. In your shift, which ones among the five items would need development the most?
5. How would it be possible to develop performance on these items?
6. What new did you learn during the exercise?
7. Stress is a natural part of a difficult situation. Stress can enhance performance, while too much stress may have negative effects. What kind of things caused stress during the exercise?

3.4 Analysing the method use

For a descriptive analysis of the group self-evaluations the recorded group discussions were considered in view of two categories, these being 1) 'reflection' and 2) 'developmental reflection'. This categorization was made by 'episodes', that is, short sequences in discussion regarding a common subject. Reflection here means talk where the operators are analysing or commenting on themes prompted by their simulation experience or by the self-evaluation guideline. Reflection is expressed as uncertainty or doubt, dilemmatic speech, expressions of challenges, evaluation or questioning, and expressions of feelings (Heikkilä & Seppänen, 2014). The second category (which is a subcategory for the first one) involves reflection that can be considered to generate new work practices or modify the existing ones. It involves collective generation of new work practices through discovery, analysis, novel perspectives and mutual commitment on developing work practices. In view of education theory, this latter category was inspired by the concept of 'transformative agency' wherein individuals are decidedly able to make changes in their work activity (Heikkilä & Seppänen, 2014).

4 RESULTS

The 'reflection' category was quite abundant in the evaluative group discussions carried out after the simulation training and individual evaluation, consisting of 33 episodes and about 62% of all discussion in words. Most of them, 20 episodes, dealt with shifts' performance during simulation. For instance, the mutual communication among the shift was a theme of discussion as in the example below:

[a] Operator 1: *Yes, so that even if both have things going on and in hurry, there should be half minute time to go through what has happened and was done; surely already when tried to reach you with the phone told what is the situation* [in the simulator scenario, one of the operators was outside the operating room during the incident]

[b] Operator 2: *On the other hand, with these flow chart procedures it is easy to jump into action*

[c] Operator 1: *So that we are there now* [certain point in the flow chart]

[d] Operator 2: *It is clear and easy after all*

One third of the 33 reflective episodes (11 episodes) were categorized as 'developmental reflection'. They differ from 'regular reflection' in that in addition to mere questioning and evaluation, new perspectives to work practices are generated collectively. Differentiation between these two categories was at times difficult and therefore the prevalence indicated here should be considered only as a rough description of the data. (For instance, the example above could be seen as 'developmental reflection' and to involve some elements that could enhance work practices – see quotation [a] in the excerpt above – but the episode was nevertheless categorized as regular reflection, because development ideas were voiced fleetingly and there was lack of consensus among the operators: the suggestion in quotation [a] was negated in the quotation [b].)

Overall, there was a vivid discussion among the operator shifts encompassing relevant themes, such as, work practices, collaboration, plant dynamics and stress at emergency situations. Table 1 provides an overview of types of episodes in discussion that could be beneficial in enhancing work practices in view of being categorized as 'developmental reflection'.

Table 12. *Examples of 'developmental reflection', i.e., types of discussions that could enhance work practices*

Categories	Description	Example (excerpt from a longer episode)
1. Discovering the causes of imperfect performance	Explications as to why the shift's performance was not perfect	*But that two-way communication to ensure that others have heard, it is for that you acknowledge that it has gone through. Well, as we are here very nearby anyway and the control centre is quite small, so you also see that it goes through. But of course that it* [communicated issue] *comes back, is the right way. Sometimes it remains unsaid.*
2. Commitment to improvements	Agreements on how to improve work practices	*Let's declare that from now on we will read all valve codes by spelling each letter.*
3. Analyzing the purpose of tasks	Considerations regarding the used evaluation technique (could enhance work practices trough enhancing training)	*Here comes the common thing of the shift, how we acted together and how we resolved it, mutual assessment could be the key issue.*
4. A novel perspective to tasks	Looking at performance from the point of stress (an issue usually not discussed by the operators)	Operator 1: *Well, I put here that there are many tasks, so overlapping tasks* [that cause stress] Operator 2: *Well, yes.* Operator 1: *And their prioritization that which one I do first.*

5 DISCUSSION

We have designed a self-evaluation method for supporting system resilience: it involves dialogue and reflection among operator crews about their own work practices and capability in emergency situations directly after simulator training sessions. Our preliminary analysis point towards this being a useful training procedure and the collaborating organization was supportive of it.

In developing the method, we drew from the ideas of the Finnish Change Laboratory tradition (Virkkunen & Newnham, 2013) and the French Activity Clinic (Clot, 2009). For practical reasons, the Activity Clinic's idea of self-confrontation could not be fully actualized: in discussions with the power plant representatives, it was concluded that videotaping the simulator sessions and showing clips of these sessions for the operators would be too time-consuming for the power plant organization – a specialist would be needed analysing the simulator sessions and editing the relevant clips from the tapes. This could be actualized by researchers outside intervention in a single try-out but the method would not become part of the training repertoire at the energy company organization. (However, it is our understanding that a training procedure of this kind is applied at some nuclear power plants, perhaps because it is required by the authorities.)

The starting point of our project was the empirical finding (Savioja et al., 2014) that not all operator shifts use procedures the same manner as some seem more interpretive than others, a feature that is assumed to promote system resilience. Our study is incomplete in confirming that the method would produce enhanced resilience through more interpretive work practices. Nonetheless, the results of the analysis of the discussions induced by our method seem promising. Much of the content of the reflective discussion is in line with the factors in work practices that are considered to promote resilience. As defined by the existing literature (Norros et al., 2015) 'interpretive practice', which assumedly promotes system resilience, involves appropriate dialogue, understanding of plant dynamics and lack of 'blind' reliance of procedures – all these issues were present in the discussions. Generally, the findings suggest that the notion of 'developmental reflection' could be beneficial in developing training that supports interpretive practice and system resilience: the categories found (see Table 1) could be seen as providing relevant educational aims for development and evaluation.

Acknowledgements

The study was supported by the SAFIR2018 programme, the Finnish State Nuclear Waste Management Fund (VYR), VTT Technical Research Centre of Finland, and Finnish Institute of Occupational Health, FIOH. We would also like to thank the participating operators at the Loviisa Nuclear Power Plant.

REFERENCES

Clot, Y. (2009). *Clinic of activity: the dialogue as an instrument.* In A. Sannino, H. Daniels, & K. Gutiérrez (Eds.), Learning and expanding with activity theory (pp. 286–302). Cambridge, UK: Cambridge University Press.

Gotcheva, N., Oedewald, P., Wahlström, M., & Macchi, L. (2016). Cultural features of design and shared learning for safety: A Nordic nuclear industry perspective. *Safety Science, 81,* 90-98.

Heikkilä, H., & Seppänen, L. (2014). Examining Developmental Dialogue: the Emergence of Transformative Agency. *Outlines: Critical Practice Studies, 15*, 5-30.

Hollnagel, E., Woods, D., & Leveson, N. (2007). Resilience engineering: Concepts and precepts. Hampshire, UK: Ashgate.

Macchi, L., Gotcheva, N., Alm, H., Osvalder, A.-L., Pietikäinen, E., Oedewald, P., Wahlström, M., Liinasuo, M., Savioja, P. (2014). *Improving design processes in the nuclear domain – Insights on organisational challenges from safety culture and resilience engineering perspectives.* NKS (Nordic Nuclear Safety Research) Article Series Vol. NKS-301.

Macchi, L., Pietikäinen, E., Liinasuo, M., Savioja, P., Reiman, T., Wahlström, M., Kahlbom, U., & Rollenhagen, C. (2013). *Safety culture in design.* NKS (Nordic Nuclear Safety Research) Article Series Vol. NKS-278.

Norros, L., Savioja, P., & Koskinen, H. (2015). *Core-Task Design: A Practice-Theory Approach to Human Factors. Synthesis Lectures on Human-Centered Informatics.* Milton Keynes, UK: Morgan & Claypool.

Pakarinen, S., Korpela, J., Torniainen, J., Laarni, J., & Karvonen, H. (2016). Control Room Operator Stress and Cardiac Activity in Simulated Incident and Accident Situations. In Proceedings of Enlarged Halden Group Meeting (EHPG), May 8-13, Sandefjord, Norway.

Savioja, P., Norros, L., Salo, L., & Aaltonen, I. (2014). Identifying resilience in proceduralised accident management activity of NPP operating crews. *Safety Science, 68,* 258-274.

Seppänen, L., Kloetzer, L., Riikonen, J., & Wahlström, M. (2016). A Developmental Perspective to Studying Objects in Robotic Surgery. In: Introna L., Kavanagh D., Kelly S., Orlikowski W., Scott S. (Eds.) Beyond Interpretivism? New Encounters with Technology and Organization. IS&O 2016. IFIP Advances in Information and Communication Technology, vol 489. Springer, Cham

Virkkunen, J., & Newnham, D. (2013). *The Change Laboratory: A tool for collaborative development of work and education.* Rotterdam, NL: Sense Publishers.

Wahlström, M. & Kuula, T. (2016). Organizational self-determination and new digital self-study applications as means for developing nuclear power plant operation training. In: Zaphiris P., Ioannou A. (eds) *Learning and Collaboration Technologies. LCT 2016. Lecture Notes in Computer Science, vol 9753*. Cham, CH: Springer.

Oral Presentations’ Abstracts

Oral presentations

Critical Infrastructure, Resilience & Governance

A CAPABILITIES APPROACH TOWARDS PRIORITIZATION OF CRITICAL INFRASTRUCTURE RESILIENCE

Susan Clark[1], Thomas Seager[2]

[1] Arizona State University - ASU (USA) (ASU) – susan.spierre@asu.edu, United States

[2] Arizona State University - ASU (USA) – United States

In response to extreme weather events, terrorist and cyber-attacks, as well as other lowprobability, high consequence technological catastrophes, recent policy directives and capital investments have exhibited a shift in priorities for critical infrastructure systems that emphasizes resilience. As a part of this resilience effort, the U.S. Department of Homeland Security (DHS) has identified 16 distinct critical infrastructure areas that are considered vital to the nation's security, economy, and/or health and safety. However, there remains no articulated set of values that guides decision-makers about the prioritization of resilience investments towardsone critical sector over another, which is particularly important in the event of a disaster. To assess the order in which we value infrastructure, we must consider why we have infrastructure and what it does. At the most basic level, infrastructure is valued because it helps people thrive and prosper; Infrastructure helps individuals and households reduce costs, increase productivity, increases the quality of health and education services, as well as facilitates social cohesion. Thus, we argue that decisions about infrastructure priorities and investments affect not only national security and the economy, but also the lives and livelihoods of people as individuals and the collective. The failure of infrastructure to provide services can therefore restrict agency, prevent people from doing things they value, and undermine their ability to cope with threats. This view emphasizes that the importance of infrastructure is to provide critical services to the public and begs the question of what services are critical to meet basic human needs and the collective values of the public.

Our collective values are often written into law. For example, the Declaration of Independence and the US Constitution explicitly express what values we have as Americans and what we believe to be our inalienable human rights. However, these human rights require infrastructure to be realized, otherwise they are simply ideas. For example, the right to life cannot be achieved without access to clean water, food, and healthcare. Also shelter, freedom to assemble, and freedom of expression cannot exist without the technological platforms that make exercise of these fundamental human rights possible. Therefore, critical infrastructure can be defined as those systems that provide us with the capabilities to actualize our human rights and prioritization can be established via hierarchies of human development needs. This research examines the DHS designation of criticality from a capabilities perspective and argues for a capabilities basis for making distinctions between those systems that should be considered most critical and those that might be temporarily sacrificed.

The capabilities framework is particularly useful for prioritizing critical infrastructure systems at the collective level in a way that emphasizes the role that infrastructure plays in enabling people to thrive as well as adapt to all kinds of adverse events. It can also be applied at the community level, as a framework for guiding local policy and initiatives around specific value systems.

Keywords: critical infrastructure, human development, capabilities approach, human rights, criticality

CRITICAL INFRASTRUCTURE RESILIENCE: BRIDGING THE GAP BETWEEN MEASURING AND GOVERNANCE

Hanneke Duijnhoven[1]

[1] TNO [Pays-Bas] (TNO) – Lange Kleiweg 137 2288 GJ Rijswijk, Netherlands

In this paper we review the current application of the resilience concept in the domain of critical infrastructure research and policy. The field of Critical Infrastructure research has traditionally focused on the protection and reliability of infrastructure systems in light of different causes of disturbances. Recently, a shift can be observed from a focus on the protection of critical infrastructures towards a focus on critical infrastructure resilience. We discuss the main differences between practice-based and attribute-based[i] approaches towards measuring and assessing resilience of critical infrastructure. We will address the underlying conceptualization and operationalization of (critical infrastructure) resilience and relate this to the state-of-the-art of Resilience Engineering[ii]. We discuss the implications of these different approaches with regard to their scientific merits and their practical applicability. We will argue that both types of approaches have stronger and weaker points, but in general, the field of critical infrastructure resilience would benefit more integrative perspectives and multidisciplinary embedding. In particular for the governance of critical infrastructure resilience (both in terms of policy and strategies for increasing resilience of CI). Given the nature of the domain, with a large number of actors involved and complex networks of dependencies, increasing resilience is not something that is easily achieved. One of the main challenges for the governance of critical infrastructure strategies is the large, varied network of public and private stakeholders involved in combination with the connectivity, complexity and dependencies within the network of infrastructure systems. The existing approaches in the field of CI research generally have a rather narrow interpretation for resilience as the ratio of loss and recovery in the face of a disturbance. The performance-based approaches have a scientific orientation, but generally do not provide insights that contribute to the governance of CI resilience. Many attribute-based approaches provide some direction as to what type of capacities a system should strive for, but assessments are rather subjective and it does not guarantee that it constitutes sustainable capacity in changing circumstances. What is more, most of these approaches are targeting single organizations or infrastructure systems, while from a governance perspective it is relevant to address resilience at the level of the network or even at the societal level. As such, the field would benefit from an integrated, network-level, approach that is rooted in scientific knowledge, while at the same time providing insights that truly contribute to the governance of critical infrastructure resilience.

[i] Vugrin, E. D. (2016). Critical Infrastructure Resilience. In IRGC, Resource guide on resilience (v.29-07-2016). Lausanne: EPFL International Risk Governance Center.

[ii] Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 141, 5-9

Keywords: Resilience Assessment, Critical Infrastructure, Governance

FROM AIR TO GROUND – RESILIENT STRATEGIES AND INNOVATION ACROSS CRITICAL INFRASTRUCTURES

Ivonne Herrera[1], Beth Lay, Karen Cardiff [2]

[1] Norwegian University of Science and Technology (NTNU), Department of Industrial Economics and Technology Management – Norway 2 Consultant, Health Care – Canada

ivonne.a.herrera@ntnu.no

In this paper we compare strategies and tactics for increasing resilience in four critical domains: aviation, power generation, healthcare, and oil and gas production. We explore similarities and differences between these domains and what these mean for the application of Resilience Engineering (RE). For example, we plan to answer the following questions: What does resilience look like in everyday operations in an air traffic control center, a power plant control room, and an acute care hospital? How does each setting anticipate, prepare and respond to surprising and novel events? Are there strategies that are uniquely suited to each domain, and why? To what extent is there overlap and are there opportunities for cross learning. Which strategies would work across domains? Which would not and why? We will synthesize the current and emerging ideas to develop a set of RE themes, drawing from our respective practices and the work of international opinion leaders in RE (Woods. 2006-2016), Hollnagel, (2006-2017) and output from the recent European Project and Programmes. We believe that a set of themes is necessary to introduce RE to novices and to provide a structure for those who desire to design and operate resilient systems. As such, this paper will be part primer for the RE novice, and part ”how to” guide for RE practitioners. The authors disclose a self-serving motive of learning from each other thereby building a richer toolbox for all RE practitioners. The themes will consider the challenge of implementation and thus be paired with innovation techniques that could be used to co-create robust solutions with end-users. The direct involvement of end-users aims to bring concepts closer to practical application and with the development of operationally valid tools or processes will help organizations and systems better understand everyday work, and prepare them to function in a resilient manner. This creates an opportunity for innovative thinking at all levels of the organization with respect to preparing for, and responding to novel and surprising events. Management innovation to mature resilience concepts gives room for unique and unorthodox approaches to unleash people's thinking and attitudes; where everybody is pushed to consider useful solutions.

We have conducted systematic, structured literature reviews. There are salient concepts across the resilience literature in general, and specific concepts from RE in particular. These concepts are described by Hollnagel (2017) [1] as the ”potentials” to anticipate, monitor, respond and learn; and, by Woods (2015) [2] as graceful extensibility and sustained adaptability, flexibility, diversity, work as imagined and work as done. Our work addresses the need to further develop these concepts into practical solutions and provides a way forward based on our practice and the input of end-users.

We will present the themes and the tools to support a paradigm shift to a resilience-oriented perspective based on RE and complemented by other relevant fields of research and practice.

[1] Hollnagel, E. (2017) Safety II in Practice: Developing the resilience potentials.

[2] Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 141, 5–9.

ORGANIZING PROCESSES OF RESILIENT ORGANIZATIONS

Margaret Hinrichs[1], Daniel Eisenberg [1], Thomas Seager [1]

[1] Arizona State University (ASU) – United States

mhinrich@asu.edu

The definition of resilience which is most relevant for our examination of the interdependence between technical and human systems is that of graceful extensibility, which asks, ”How do systems stretch to handle surprises?”[1] To assess an organization’s capacity for graceful extensibility, we borrow the notion of ”agility” from the Command and Control Research Program (CCRP) within the United States Department of Defense [2] which defines ”agility” as the ability to successfully cope with and/or exploit a change in circumstances. The CCRP’s goal is to transform how people in military and civilian contexts interact and pursue collaborative endeavors in the Information Age, and to identify the conditions and technologies which enable members’ organization, synthesis, and implementation of diverse knowledge. Organizations are considered agile if they can both recognize the dynamic nature of a situation and enact the appropriate response. An organization’s capacity for agility relies upon three dimensions:

1. Patterns of interaction-the willingness and ability of members to communicate.

2. Allocation of decision rights-the distribution of power to incur decision costs.

3. Distribution of information-the extent to which information is accessible and available.

The broadest enactment of these three organizational dimensions supports processes of both tacit and explicit knowledge sharing, the result of which is increased group tacit knowledge [3] and collective improvisation regarding the use and operation of technological systems, as well as self-organizing task clusters in the face of unforeseen change to which an organization must adapt. Enactment of resilience potential thus requires communication practices and protocols which are conducive to creating and sharing tacit knowledge, empowering members to act and make decisions on behalf of the organization, and providing access to and distributing information. Implementing and rewarding such communication practices often requires changes in organizational culture which reframe who and what is valued, redefine the self in relation to others and the enterprise, and identify and clarify individuals’ motivations for action.

However, a key limitation of the CCRP’s claims regarding components of organizational agility and maturity is that they have been developed and tested in one particular kind of culture-the United States military. In addition, graceful extensibility has not explicitly examined the influence of culture on the interplay between human and technical systems. What is therefore required is a test of how the three dimensions described above constitute culture in civilian multi-sectoral organizations, and the extent to which the ensuing culture supports the creation and transfer of tacit knowledge among groups. We test the hypothesis that organizations with greater group tacit knowledge can achieve greater graceful extensibility than their counterparts. In particular, we examine organizations which must confront uncertainty and surprise regarding technology and infrastructure systems.

[1] Woods, D.D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering System Safety.

[2] Alberts, D. S., & Hayes, R. E. (2003). Power to the edge: Command, control in the information age. CCRP Publication Series.

[3] Erden, Z., et al. (2008). The quality of group tacit knowledge. Journal of Strategic Information Systems, 17(1), 4-18

Keywords: organizational culture, tacit knowledge, graceful extensibility, communication

SUSTAINED ADAPTABILITY: THE TRANSACTION LEVEL

Jan Maarten Schraagen[1]

[1] TNO [Pays-Bas] – Netherlands

Recent advances in the study of resilience engineering have focused on discovering architectures that can sustain adaptability (Woods, 2015[1]). Tangled Layered Networks show 'graceful extensibility' in successful cases of sustained adaptability, that is, these networks have the ability to extend their capacity to adapt when surprise events challenge their boundaries. A key concept in this view is 'adaptation', which includes adjusting behaviour and changing priorities in the pursuit of goals. As surprise occurs continuously, units within the network constantly need to monitor their environment and regulate their resources, in joint coordination with other interdependent units in the network. For both human and artificial systems, knowledge is one of the most important resources adaptive units can bring to bear. Any system that fluently applies knowledge in the service of goals operates at what Newell (1982[2]) has termed the 'knowledge level'. At the 'knowledge level', the principle of rationality applies: if an agent (e.g., an expert) has a goal and knows that knowledge A will bring him or her closer to that goal, then the agent will choose knowledge A. As knowledge is always finite (principle of bounded rationality; Simon, 1955[3]), adaptation can only be local and perspectives of any unit in the network are bounded. In Newell's (1982) terms, the 'knowledge level' is a radical approximation, that is, entire ranges of behaviour may not be describable at the knowledge level, but only in terms of systems at a lower level, i.e. the cognitive level.

However, if knowledge is finite, the only way for Tangled Layered Networks to show graceful extensibility is by aligning and coordinating across multiple interdependent units in a network, by shifting and contrasting over multiple perspectives, hence by extending the range of adaptive behaviour of other units. I will argue that this, in effect, calls for a different system level, right above the knowledge level, which I will call the 'transaction level'.

At the transaction level, links are selected by agents (units) to attain transactions. Architectures for sustained adaptability need to be couched in terms of the transaction level, because of the fundamental limitations at the knowledge level. Unlike Munchhausen, we cannot attain graceful extensibility by pulling ourselves up by our own hair, that is, by using concepts from the level we are trying to explain. What this means in practice is that we need to study the links between the units in the network, the information flows between the links, and discover patterns in these flows. Whereas adaptation is a goal-oriented concept at the knowledge level, it needs to be described in terms of information flows at the transaction level. Resilience engineering needs to study, then, the ways these information flows can be optimized across the entire Tangled Layered Network. In this paper, I will present a number of examples of how this can be achieved. This will be achieved partly by re-framing a number of classic disasters in terms of the transaction level, partly by recounting successful cases of sustained adaptability

RESILIENCE AND GOVERNANCE IN COMPLEX TEMPORARY ORGANIZATIONS

Dianka Zuiderwijk[1], Peter Groenewegen[1], F. Kees Boersma[1]

[1] Vrije Universiteit (VU), Social Sciences, Department of Organization Sciences – Netherlands

d.c.zuiderwijk@vu.nl

In complex organizations, no single individual has a complete understanding of the whole situation. Here, performance depends on seamless teamwork, which requires adequate organizational conditions driving a collaborative mindset, particularly in volatile and safety-critical environments. In complex temporary organizations, this effort competes with the participating permanent organizations' objectives and is influenced by each organization's unique signature [1], relating to for instance political pressures, pace and synchronization, as well as internal commercial targets, reward systems and commitments to other projects. Temporary organizations are a growing phenomenon across many sectors. It refers to entities formed by multiple organizations, each contributing a part of the scope required to achieve the temporary organization's objective. The inter-organizational dynamics differ from intraorganizational dynamics [2] since temporary organizations are also influenced by the permanent organizations' internal motivations, e.g. how high is the specific project contribution on the internal priority list of the permanent organization? Moreover, the contributions may be (partly) subcontracted to other organizations which, in turn, may subcontract pockets to yet other organizations creating a constellation of mixed interests. The success of a temporary organization is influenced by the resilience capability at the point where contributions come together in design, realization and operation, as actors from different disciplines and from different organizations navigate through the situation together [3], adapting 'work as imagined' to the reality of work as it manifests itself while coping with the inevitable gaps on the seams between their contributions and their permanent organizations' priorities.

This project has a special focus on the effect of the regulatory governance approach on the resilience capability in temporary complex organizations. While organizations become more complex, the regulator simultaneously increases the emphasis on rule compliance, which seems a counterintuitive move.

Exploratory data capture at industry partners of the dynamics and resilience in temporary organizations in different sectors allows for a discussion on cross-sectorial patterns, developing an understanding of how different sectors cope resiliently with the dynamics in temporary organizations under increasing compliance pressure. While TORC (Training for Operational Resilience Capabilities) [4] created an understanding of how resilience works within one organization, this paper aims to explore how resilience works between organizations engaging in a temporary complex organization.

[1] Berkel Ferguson, J.E., Groenewegen, P., F. J. F. W. van. (2016). Speedy Delivery Versus Longterm Objectives: How Time Pressure Affects Coordination Between Temporary Projects and Permanent Organizations. Long Range Planning

[2] Berthod O. Muller-Seitz, G., Raab, J., Sydow, J., G.-H. M. (2016). From High-Reliability Organizations to High-Reliability Networks: The Dynamcis of Network Governance in the Face of Emergency. Harvard Journal of Public Administration Research and Theory, (1–20)

[3] Stacey, R. (2012). Tools and Techniques of Leadership and Management: Meeting the Challenge of Complexity. Abingdon: Routledge

[4] Grotan, T.O., Waero, I., Van der Vorm, J., Van der Beek, D., Zuiderwijk, D. (2016). Using gaming and resilience engineering principles to energize a situated resilience training of front-end operators and managers, Safera, delivered at the ESREL Conference Glasgow, September 2016

Oral Presentations

Health Care Systems

EMERGENCY MEDICAL SERVICES: WHEN FATIGUE BECOMES THE NORM

Pierre Bérastégui[1,2], Mathieu Jaspar [3], Anne-Sophie Nyssen [3,4], Alexandre Ghuysen [4]

[1] Laboratoire d'Ergonomie Cognitive et d'Intervention au Travail (LECIT) – Belgium

[2] Centre de Simulation Médicale Interdisciplinaire de Liège (SMILE) – Belgium

[3] Laboratoire d'Ergonomie Cognitive et d'Intervention au Travail (LECIT) – Belgium

[4] Centre de Simulation Médicale Interdisciplinaire de Liège (SMILE) – Belgium

BACKROUND: Emergency Medical Services (EMS) routinely work at the very limit of their capacity due to growing emergency rooms visits and residents' shortage. In this context, EMS workers are regularly asked to work more than 10 hours a day, on varying shifts and with short recuperation breaks. Two approaches can be used to reduce fatigue-related risk: reducing the likelihood a fatigued operator is working (i.e. fatigue reduction), or reducing the likelihood a fatigued operator will make an error (i.e. fatigue proofing). In Emergency Medical Services, formal risk control mainly focuses on reduction strategies such as reducing work hours while proofing strategies develops as an implicit element of the safety system.

OBJECTIVE: Our purpose is to identify individual proofing and reduction strategies used by emergency residents and to investigate how they relate to fatigue, performance and patient safety indicators.

METHODS: First, we conducted 4 focus-group sessions with a total of 25 EMS residents to elicit perceived consequences of fatigue and strategies used to cope with them. Focus group results were used to design a questionnaire assessing how often EMS residents personally used any of the strategies reported during sessions. Second, we administered the questionnaire to a larger sample and conducted a prospective observational study with a repeated within-subjects component. A total of 45 EMS residents participated in the study for a total of 400 shifts analyzed. We gathered sleep diaries, subjective sleepiness, reaction time, self-reported medical errors and performance ratings at different time point during both day and night shift using an android-based application. Sleep time and activity levels were confirmed using wrist actigraphy.

DISCUSSION: We will discuss what can be drawn from our results in terms of individual and collective resilience processes with a focus on the potential for implementation of more formal processes at a system level.

Keywords: Fatigue, Risk, Resilience, EMS, Residency, Patient Safety

WORK-AS-DONE TO INFORM PROTOCOL DEVELOPMENT IN THE EMERGENCY DEPARTMENT

Katherine Forsyth [1], Rachelen Varghese [2], Nibras El-Sherif [1], Hunter Hawthorne [1], Renaldo Blocker [1]

[1] Department of Health Sciences Research [Mayo Clinic] (HSR) – Mayo Clinic 200 First Street SW Rochester, MN 55905 USA, United States 2 Department of Emergency Medicine [Mayo Clinic] (EM) – Mayo Clinic 200 First Street SW Rochester, MN 55905 USA, United States

Introduction: The emergency department (ED) is a dynamic environment that requires providing timely care to patients of varying acuity. Many times, clinicians don't follow protocol because it does not adquatenly represent their everyday workflow. This discrepancy results in the development of workarounds and/or unofficial protocols to communicate critical information or perform time senstive tasks. However, varying protocols for tasks can disrupt one's workflow, cause confusion and lead to errors impacting patient safety. The present study sought to use observations to identify tasks occuring in-situ as a source of evaluating work-as-done in the ED in order to identify opportunities to bridge the gap between protocols (i.e., work-as-imagined) and clinical work (i.e., work-as-done). Method: Attending physicians at one academic institution were observed and workflow tasks were identified. Convenience sampling was used to select the physicians in the ED to observed. Data included a description of the task, who were engaged in the task (e.g., nurse, resident, technologist), and the location (pediatric or adult wing). Insitutional procedures were reviewed for each task to identify whether relevant protocol was in place. For those lacking relevant protocol, the tasks annotations were categorized according to opportunities for protocol creation.

Results: During two attending physician shifts, 22 tasks were identified. 55% of the tasks were conducted by nurses, 23% were conducted by residents, 14% were conducted by radiology and 9% were conducted by other staff. There were 17 (77%) tasks identified as "Work As Done" (WAD) that did not have a formal protocol associated with the task. There were 5 (23%) tasks identified as Work As Imagined (WAI) that had a formal protocol associated with it and clinicians followed the protocol. Of the 77% WAD there are opportunity for protocol development related to continued patient care processes (53%), clinician administrative processes (29%) and clinician training processes (18%). Discussion: A majority of the tasks identified in this study lacked associated protocol. Creating procedures for continued patient care processes, clinician administrative processes, and clinician training processes using work-as-done data will provide a chance to build resiliency into the work system. Developing procedures from the ground up (i.e., sharp end) rather than enforcing procedures that come from the top down (i.e., blunt end) will ensure that protocols can be flexible for performance adjustments and unexpected events when they arise. Next steps will include: 1) interviewing ED clinicians on their workflows for particular tasks, and 2) developing relevant and safe protocols alongside affected clinicians so that the protocols are an accurate representation of everyday work.

Keywords: work as done, work as imagined, emergency department, protocol development

ADAPTATION AND IMPLEMENTATION OF THE RESILIENCE ASSESSMENT GRID IN AN URBAN EMERGENCY DEPARTMENT

Garth Hunte[1]

[1] The University of British Columbia [Vancouver] (UBC) – Canada

SUMMARY We adapted the generic Resilience Assessment Grid[i] to the emergency department (ED) context, and implemented a context-specific instrument to rate and monitor the everyday way an urban ED copes with the challenges and trade-offs that arise in risk critical work.

The context-specific instrument was derived from a series of dialogue workshops in a practice community of patients, care providers, support staff, and leaders. Workshops were based on the World Caf´e strategy, and used statements from the generic Resilience Analysis Grid cas a stimulus. Diagnostic statements were refined in monthly inter-professional departmental workshops for content and face validity, then used to plot a departmental resilience profile.

Through conversation and stories of everyday practice participants populated context specific examples of how the department and local healthcare system responds to what happens, monitors critical threats, learns from what happens, and anticipates what might happen.

The iterative work-in-progress of engagement and dialogue within a practice community using the generic Resilience Assessment Grid c as a stimulus for dialogue and action has been generative in identifying gaps and actions to increase collective adaptive capacity. For example, statements about 'vital signs', thresholds and action plans have led to parallel work on the suite of operational metrics that practitioners and staff look at to get a sense of how the ED is operating. The ED Operational Vital Signs have been implemented locally in an hourly printout version, and an integrated electronic version is anticipated in the new few months.

Repeated application of the Resilience Assessment Grid **C** over time demonstrates how the profile of a resilience potential develops and enables systematic monitoring and evaluation of specifically targeted efforts. The tool has been refined to create a context-specific strategic framework with face and content validity. The process created community, identified gaps, and has led to innovations and actions to increase collective capacity for manoeuvre. The ED resilience profile will continue to be iteratively mapped over time.

RELEVANCE FOR SYMPOSIUM

The process of adapting and implementing the ED context-specific Resilience Assessment Grid has provided a space for practitioners, patients, and leaders to share in a conversation together about where we are and where we want and need to go. It has led to critical conversations about how patients are cared for safely in a complex clinical environment, and to consideration of how to adapt and respond to crowding while maintaing a safety margin and capacity for manoeuvre.

SIGNIFICANCE/TAKEAWAY

There was value in adapting the generic Resilience Assessment Grid to a local healthcare context in bringing a diverse group of clinicians, staff, patients and leaders together to focus on a systems view of complexity in everyday work. Industry and science can follow a similar methodology rooted in Appreciative Inquiry and complexity-based models of meaningful engagement to facilitate and foster a dialogue about how resilience potentials emerge and can be supported.

[i] Hollnagel E. Epilogue: RAG – the Resilience Analysis Grid. In: Resilience Engineering in practice: a guidebook. Ashgate Publishing Limited; 2011. p. 275–296.

Keywords: Resilience Assessment Grid, healthcare, emergency department

RESILIENCE: THE CHALLENGE OF MAINTAINING MARGIN IN HEALTHCARE

Mary Patterson[1], Ellen Deutsch [2], Rolin Fairbanks[3], Robert Wears[4]

[1] Children's National Medical Center – 111 Michigan Ave NW Washington, DC 20010, United States

[2] Pennsylvania Patient Safety Authority and ECRI Institute – Patient Safety Authority 333 Market Street Lobby Level Harrisburg, PA 17120, United States

[3] National Center for Human Factors in Healthcare; Medstar Institute for Innovation – 3007 Tilden St NW 7, Washington, DC 20008, United States

[4] University of Florida and Imperial College – 655 W 8th St, Jacksonville, FL 32209, United States

At first glance, safety practitioners new to the field of reliance engineering may automatically view Safety I as a reactive approach and Safety II as a proactive approach. This is understandable as Safety I often involves a response to an incident or adverse event while Safety II is concerned with adaptation and flexibility. However, in thinking more deeply about these concepts, this ”either / or” assignment is artificial and inconsistent with actual practice. We propose to discuss reactive and proactive approaches to Safety I and Safety II using safety events in healthcare (unsafe conditions, incidents and serious events) as exemplars. Constructs such as reactive and proactive are less helpful in understanding Safety I and Safety II and alternative frames may be useful.

In considering Safety I, root cause analyses, training, and creating policies in response to an incident are consistent with a reactive approach. Alternatively, implementing forcing functions and standardized rules to minimize variation can be a proactive approach to safety, albeit from a Safety I perspective focused on anticipated failures. (Vincent and Almaberti 2016). However, we can also identify Safety II approaches that are both reactive and proactive. A reactive Safety II activity might include examination of ”normal cases” in association with unsuccessful cases of the same type. For example, when investigating cases in which spinal cord compression was missed, a large number of cases in which spinal cord compression was appropriately diagnosed and managed were also reviewed. A proactive safety II approach might include preparation of resources (personnel, equipment, processes) and margin in anticipation of a threat. Ensuring that personnel have the appropriate skill sets and familiarity with a system before they are required to function in the system is another proactive approach. Perhaps a better differentiation is that Safety-I tends to restrict operators' capabilities, Safety-II tends to expand them. The Safety II approach might better be when the operator is ”poised to adapt”: possessing a deep knowledge of the situation, system and resources. (Cook, 2016) Alternatively, one might consider Safety II as ”training for flexibility in the face of the unexpected rather than for specific threats” (Finkel, 2011).

RELEVANCE

Creating the space for resilience to occur requires that resources to facilitate adaptation are maintained at a level that allows for graceful extensibility (Woods, 2014) rather than constant ”firefighting mode” (Schulman and Roe 2004). Ensuring adequate margin may be viewed as a radical philosophy in an era of ”rightsizing” and Lean. SIGNIFICANCE/TAKEAWAY The consequences of insufficient resources for adaptation in the face of unexpected perturbations may not be immediately apparent. In fact, the system may continue to function adequately until a crisis challenges the system's operations. In the case of healthcare, surges in patient census and unusually challenging patient conditions (e.g. ebola) represent regular and irregular threats to operations. Critical system failures may be precipitated by inadequate availability of resources necessary for system adaptation. Lack of sufficient margin to respond to perturbations may in itself be a latent or unsafe condition.

Keywords: margin, proactive, reactive, healthcare, safety II

WHAT IS A STEP IN THE RIGHT DIRECTION? THE TRADEOff BETWEEN IMPROVING IDEAS AND IMPROVING SYSTEMS

Michael Rayo[1], Rollin Fairbanks [2]

[1] The Ohio State University, Columbus, OH, USA – United States

[2] MedStar Institute for Innovation, Washington, DC, USA – United States

We will be discussing, and perhaps debating, how to discern the true indicators of true progress in the larger safety and system performance communities with respect to adoption of Resilience Engineering concepts and precepts (i.e., ”steps in the right direction”). There is a long and painful tradition of Resilience Engineering being misinterpreted, misunderstood, and co-opted into more mainstream theories, most notably Root Cause Analysis and the other theories that Hollnagel, et. al. has aggregated under the label of Safety I[1]. Ultimately, this has stunted the progress of Resilience Engineering specifically and of engineered system resilience in general. It also creates a difficult decision among resilience engineers as to how to direct their efforts: which of the updated, amended, or ostensibly brand new perspectives of system safety and performance should we support? Which should we tolerate because one or more aspects are better than the status quo? Which should we actively resist and criticize? Which should we co-opt and exploit, even if our interpretation does not match the original designers'? Perhaps most importantly, how should we approach the tradeoff between engaging in these activities to support Resilience Engineering and doing work to improve the resilience of a specific system? We will discuss our recent efforts in applying Resilience Engineering in our respective health systems, and how recent large-scale safety initiatives from the Agency for Healthcare Research and Quality and the National Patient Safety Foundation may help and hinder our future efforts. As Associate Director of the MedStar Institute of Innovation as well as being an Attending Physician in the Emergency Department of the MedStar Washington Health Center, Terry Fairbanks directs how untoward events are investigated and advises the rest of the organization on how potential safety interventions should be designed and implemented. He also serves as an advisor to multiple healthcare safety organizations, helping them craft safety guidance to health systems in the United States. He will highlight the barriers that he has faced in bringing a Resilience Engineering perspective to his organization, and will discuss successes and failures in some of his recent projects. Mike Rayo will talk about his experience as an insider/outsider in his organization, with his primary appointment being in the College of Engineering but playing a consulting role in the Department of Quality and Patient Safety in The Ohio State University Wexner Medical Center. He will discuss how much of the language of Resilience Engineering concepts have adopted by more mainstream safety ideas like Root Cause Analysis, but the concepts themselves have not. He will discuss how it is important to look at the recommendations of a given investigation or guidance document, and compare them against the tenets of Safety I or Safety II. Even though our community has succeeded in including language that guides against blaming individuals and looking deeper into systemic issues, the lack of guidance on how to do this often leads well-meaning investigation teams to backslide into what is comfortable for them. He will also share his recent projects at Ohio State, and how he is slowly bringing Resilience Engineering to the consciousness of the organization through small projects that yield small, but notable, improvements.

Hollnagel, E. (2014). Safety-I and Safety-II. Ashgate Publishing, Ltd.

THE CONCEPT OF RESILIENCE IN SURGICAL OPERATIONS – FROM HANDLING DISTURBANCES TO COPING WITH COMPLEXITY, UNCERTAINTY AND CONTRADICTIONS

Mikael Wahlström [1]

[1] VTT Technical Research Centre of Finland (VTT) – Vuorimiehentie 5, FI-02150, Espoo, Finland, Finland

An established definition for resilience in health care goes as follows: 'the ability of the health care system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required performance under both expected and unexpected conditions'[i]. This definition is in line with the generic definition of resilience and is therefore likely to reflect the typical safety-critical work contexts explored in the resilience engineering literature, such as the aviation or nuclear domains. In these work contexts operators usually engage in routine tasks or monitoring while challenge-defying performance is required during disturbances. It is then quite natural to connect the concept of resilience to disturbances and changes. However, the resilience engineering literature also suggests a clear difference between health care and other safety-critical domains in that health care commonly involves abnormal situations, not previsioned in the system design or procedures. For instance, Blocker[ii] has identified that non-routine events are extremely commonplace (it was observed that there are, on average, 56 distracting, undesirable, or unusual events per cardiac-surgery case). Overall, Clay-Williams and Braithwaite[iii] illustrate the actualities of health care by suggesting that it resembles wartime military aviation in requiring flexibility and in-situ decision making.

Indeed, changes and disturbances seem to be so common that the line between so-called 'expected' and 'unexpected' could become blurred. Similarly, in some health care settings, in surgery especially, one could see that it is not primarily so that a 'change' or 'disturbance' would be something that interrupts the 'normal' course of operations. Instead, the surgical operation itself is a huge 'disturbance', introduced by the surgical team, which has to be managed and controlled, while each patient is different in terms of anatomy and disease status. Furthermore, in the context of complex surgeries, the guidelines are fairly incomprehensive and unspecific, and they entail scientific uncertainty[iv]. There is also always present a contradiction: the aim is to heal a disease while at the same time minimal damage should be introduced.

In this view, resilience in complex surgical operations is not so much about system's ability to function despite disturbances and changes (although they are relevant), but it is more about handling a complicated process despite the lack of exact scientific knowledge, the variability and complexity of human bodies, and the contradicting aims.

This work was supported by The Finnish Work Environment Fund.

i Hollnagel, E., Braithwaite, J., & Wears, R. (2013). Resilient health care. Farnham, UK: Ashgate.

ii Blocker, R. C. (2015). What can non-routine events (NRES) teach us about managing resilience? Presentation at 6th Resilience Engineering International Symposium Lisbon (Portugal), 22 – 25 June 2015.

iii Clay-Williams, R., & Braithwaite, J. (2013). Safety-II Thinking in Action: "Just in Time" Information to Support Everyday Activities. In E. Hollnagel, J. Braithwaite, & R. L. Wears (Eds.), Resilient Health Care (pp. 205–214). Farnham, UK: Ashgate.

iv Wahlstr´´om, M., Sepp´´anen, L., Norros, L., Aaltonen, I., & Riikonen, J. (submitted). Resilience through interpretive practice – A study of robotic surgery. Journal manuscript under peerreview.

Keywords: resilience, health care, surgery

Oral presentation

"Disaster" Anticipation, Response & Recovery

SUPPORTING RESILIENCE MANAGEMENT THROUGH GUIDELINES: SPECIFYING THE NATURE OF THE GUIDELINES, DEVELOPMENT PROCESS AND ESSENTIAL COMPONENTS

Matthieu Branlat[1], Rogier Woltjer [2], Luca Save [3], Odeya Cohen [4], Ivonne Herrera [1]

[1] SINTEF Digital – Strindveien 4, 7034 Trondheim, Norway

[2] FOI – Link¨oping, Sweden

[3] Deep Blue srl – Rome, Italy

[4] Ben Gurion University of the Neguev – Beer Sheva, Israel

H2020 project DARWIN aims to build resilience management guidelines to support organisations in developing and enhancing their resilience in the context of crisis management. During the first 6 months of the project, a vast review of associated literature, standards and operational documentation, as well as interviews of practitioners, was undertaken. A significant number of requirements were identified to guide the subsequent development of the DARWIN guidelines. Those requirements included especially conceptual requirements that captured resilience management capabilities the guidelines should address. However, the requirements did not specify the nature of the guidelines, i.e. the object of design, in order for them to be useful. The development of such object is a typical ”ill-defined” problem, i.e. corresponds to a problem for which there is no clear end goal, nor clear path to a solution. The nature of such problem is further complicated by the typical scope, scale and complexity of the domain of crisis management for which the guidelines are developed. The paper describes the iterative discovery process that took place in order to define the nature of the guidelines, to establish a development process and create an initial version of the guidelines. The context is that of organisations that already have a number of processes and tools in place to support their management of crises (e.g., preparation activities, contingency plans, procedures, learning activities). As a result, the guidelines are positioned at a meta-level: they provide a perspective on these processes and tools grounded in research and practice on resilience management inspired by the fields of Resilience Engineering and Community Resilience.

The guidelines are constituted of three essential components: The building blocks are the Concept Cards (CC). CCs propose specific interventions in order to develop and enhance the resilience management capabilities captured in the conceptual requirements. CCs are at the heart of the guidelines development process described in this document; they are built and revised by incorporating operational perspectives.

The guidelines build on the Concept Cards by organising and relating them, because the resilience management capabilities they refer to are not independent. A central component of the guidelines in a conceptual map that organises the CCs; it is used both for knowledge representation and development purposes. • A knowledge management platform facilitates the development, management and future use of the guidelines. The platform offers opportunities to reconsider common views on the nature of guidelines, their necessary evolution and their multi-faceted, multi-purpose content.

The guidelines' development follows a 4-step process established to be collaborative and iterative, and to include operational input early and as often as possible. The process changed and solidified during the course of the task as a result of the evolving understanding of what type and content of guidelines would be useful to develop and of how to produce such guidelines while fulfilling the various objectives of the project. Finally, the paper describes current results, achievements and limitations associated with the initial version of the resilience management guidelines.

Keywords: resilience management, guidelines, design, development, discovery process, knowledge management

SITUATED AND PARTICIPATORY DEVELOPMENT OF A COLLABORATIVE TECHNOLOGY TO IMPROVE THE RESILIENT PERFORMANCE OF DISASTER RISKS MANAGEMENT

Ricardo Carvalho[1], Paulo Carvalho[2], Ademir Silva Junior [1], Alyson Souza[1], Pit´agoras Bindé[1]

[1] Universidade Federal do Rio Grande do Norte (UFRN) – Brazil

[2] Instituto de Engenharia Nuclear do Rio de Janeiro (IEN-RJ) – Brazil

rijmatos@gmail.com; paulov195617@gmail.com; ademirbezerra2012@gmail.com; alyson@imd.ufrn.br; pitagorasjbinde@gmail.com

The Information and Communication Technologies (ITCs) designed to manage the risks of disasters presents restraints concerning the generalization of its use for they do not account for the diversity of disaster risks, the culture, the language, and the users. The current article discusses the issues related to the disaster alarm and alert system, the communication and coordination of actions referring to the disaster which occurred in 2014 in the neighborhood of M˜ae Lu´ıza in Natal- RN, Brazil. It also presents a situated and participatory development model of an application created to be used by populations vulnerable to disasters, civil defense and protection agents, and volunteers in the management of disaster risks. It was verified in the aforementioned disaster that the local alarm and alert system happened through word-ofmouth and the agents did not have anticipated access to the images and certain information of risk areas. The communication between the population and the public agents involved was not very agile, which contributed to increase the uncertainties and hampered the proper decision making, the coordination of the response actions and the performance of actions in due time. Because of that, the risks increased and the population had more difficulty to leave the risk areas in an early and quick way. It was noticed that the community had not been prepared to act in situations of risk and disaster, though they acted before and during the disaster specially, even in an unprepared way and without an integrated coordination. In some discussion forums the community pointed the need to improve the alert and alarm communication as well as the communication among the agents and the population and the action coordination. In order to accomplish that, it was suggested the creation and use of an application for mobile phones at low cost. There are several studies and researches which refer to the contribution of ITCs for that purpose but so far it has not been identified any device which has adopted the situated and participatory method of development or that refers to the focused population and location. The application is being developed with the participation of the neighborhood population and public agents, thus considering their accumulated knowledge and experience. The aim is to provide potential users with information on the risk of disasters, receive alert and alarm warnings and also guidelines on how to evacuate areas of risk safely. It is also foreseen that the application will have the following functions: social and demographic information, risk mapping, garbage mapping, disabled people, elderly, children and adolescents mapping as well as physically challenged people and their homes, the possibility of communication among users and the access to first aid procedure tutorials, the possibility to coordinate emergency actions and etc. The next steps expected are the usability test and the test and validation during a drill to be performed in the neighborhood. It is intended to use the application to contribute to the improvement of community resilience and also the city of Natal in face of disaster risks.

Keywords: disaster risks management, resilience, participatory design, situated action, collaborative technology, information and communication technology

RESILIENCE AT SCALE IN MASS CASUALTY RESPONSE(I): THE FORMOSA FUN COAST FIRE, JUNE 2015.

Sheuwen Chuang[1], David Ting [2], Richard I. Cook [3]

[1] School of Health Care Administration, Taipei Medical University (TMU) – 12F, No.172-1, Sec

[2] Keelung Rd., Taipei, Taiwan 2 Department of Neurosurgery, Taipei Hospital, Ministry of Health and Welfare – Taiwan

[3] Department of Integrated Systems Engineering, The Ohio State University – United States

The fire at the Formosa Fun Coast Park, Taiwan, had started because of a flammable, coloured powder was sprayed from a stage onto the audience around 20:30 Saturday June 27 2015. Nearly 500 young people were burned, of which 200 burned seriously and 15 had died. [Five hospitals were selected in our study for understanding how the hospitals responded to the needs from casualties and provide safe care for the injured. There are one public regional hospital, two government-owned but private operated hospitals (one medical centre and one regional hospital), one private regional hospital, and one missionary hospital (medical centre). This accumulated 144 burn patients. The proposal is to discuss the resilience characteristic of the public regional hospital at the first and intermediate moment of accepting the casualties. The ED of the public hospital has average 66 patient visits at 8:00-22:00, and 37 visits at 23:007:00 per day. They have 3 acute beds and 20 general beds. Two shifts of physician care and three shifts of nursing care are scheduled per day. One internal medicine physician and one surgical physician are allocated for each physician shift; six nurses plus one nurse practitioner are assigned for each nursing shift. 30 burn patients were transferred to the hospital during the accident. They were injured around 10 -50% of total body surface area (TBSA). They arrived in two waves: 21 patients came in every 2 minutes from 22:04 to 23:06; 8 patients came in every 3 minutes from 23:32 to 23:56, 3 were in serious conditions. The last patient came at 00:20.

The communication about how many patients could be transferred to this hospital was not clear between the Regional Emergency Medical Operation Centers(REMOC) and the hospital especially within the first 2 hours after the disaster. Although the number of transferred patients was far more than the hospital's expected based on their current capacity, the hospital performed professional responses to this event. These responses were categorized into two groups: common adaptations and special adaptations. Common adaptations indicate those changes that were commonly performed in emergency rooms elsewhere when a disaster broke out. Special adaptations are those changes acted differently from other hospitals while facing the same scenarios, because of particularly limited capacities in the organization. The study identified major five common adaptations and six special adaptations. The hospital pulled out their surge capacity by these adaptations to provide necessary care for the injured. It is a particular resilience model for a public regional hospital.

Keywords: formosa fun coast fire, mass casualty

IMPROVING URBAN INFRASTRUCTURES RESILIENCE USING CONCEPTUAL MODELS: APPLICATION OF THE ”BEHIND THE BARRIERS” MODEL TO THE flOODING OF RAIL TRANSPORT SYSTEM

Michael Gonzva [1], Bruno Barroca [1]

[1] Paris-Est University (UPEM) – Université Paris-Est : EA3482 – 5 boulevard Descartes, Champs-sur-Marne, 77454 Marne-la-Vallée Cedex 2, France, France

The vulnerability of guided transport systems facing natural hazards is a burning issue for the urban risks management. Experience feedbacks on guided transport systems show they are particularly vulnerable to natural risks, especially flood risks. Besides, the resilience concept is used as a systemic approach for making an accurate analysis of the effect of these natural risks on rail guided transport systems. In this context, several conceptual models of resilience are elaborated for presenting the various possible resilience strategies applied to urban technical systems. One of this resilience conceptual model is the so-called ”Behind The Barriers” model based on the identification of four complementary types of resilience: (i) cognitive resilience, linked to knowledge of the risk and the potential failures; (ii) functional resilience, representing the capacity of a system to protect itself from damage while continuing to provide services; (iii) correlative resilience, that characterises the relationship between service demand and the capacity of the system to respond; (iv) organisational resilience, expressing the capacity to mobilise an area much wider than the one affected.

The purpose of this paper is to offer an application of a resilience conceptual model, the ”Behind the Barriers” model, relating to a specific urban technical system, the public guided transport system, and facing a particular risk, a flood hazard. To do that, the paper is focused on a past incident on a French Intercity railway line as a studied case. Indeed, on June 18th and 19th 2013, the rise of the level of the ”Gave de Pau” river, located in the municipality of Coarraze, caused many disorders on the intercity line serving the cities of Tarbes, Pau and Lourdes. The latter is knowing as one of the world’s most important sites of pilgrimage and religious tourism. Among the disorders caused by the flooding, about 100 meters of railway embankments were collapsed. With a constraint to reopen the line before August 15th, reinforcements were studied in order to stabilize the railway embankment. During the works, substitute shuttle service was set up, providing services between cities.

This French past incident is studied through the ”Behind The Barriers” model: i. cognitive resilience: what was the level of knowledge of the stakeholders concerning the flood hazard?; ii. functional resilience: what could be done in order to maintain the railway service between the cities?

iii. correlative resilience: what was the operator’s response about the service demand with respect to the capacity of the railway line to ensure service?

iv. organizational resilience: what was the mobilization of the impacted cities, the impacted French department, the National authorities... on a wider scale than the flooded area in order to restore the line? The paper gives the main conclusions of this study and shows that resilience conceptual models such as ”Behind The Barriers” are relevant and powerful frameworks to understand damages on critical infrastructures due to natural risks.

Keywords: Risk, Resilience Conceptual Model, Rail Transport system, Floodin

UNREASONABLE EXPECTATIONS? EXAMINING THE USE OF PUBLIC TOLERANCE LEVELS AS CRITICAL INFRASTRUCTURE RESILIENCE TARGETS

Laura Petersen[1], Laure Fallou [1], Paul Reilly [2], Elisa Serafinelli [2]

[1] European-Mediterranean Seismological Centre (EMSC) – European-Mediterranean Seismological Centre – c/o CEA, Bât. BARD Centre DAM - Ile de France Bruy`eres-le-Châtel 91297 Arpajon Cedex France, France

[2] The University of Sheffield [Sheffield] – Western Bank Sheffield S10 2TN, United Kingdom

Maintaining the minimum acceptable level of service as well as the rapidly restoring full services are two components of critical infrastructure (CI) resilience that are particularly pertinent during disasters [1]. However, no consensus currently exists on what should be the minimum level of service or restoration time. For actors that meet public needs, such as CI operators, the general public's expectations and tolerance levels should be considered. Furthermore, going beyond basic needs and meeting expectations helps to maintain a good reputation in times of crisis [2]. While an ”expectation gap” between what services the public expect CI operators to provide after a disaster and what CI operators are realistically able to deliver is a recurring theme in the literature[3] [4], few of these studies have empirically investigated what members of the public expect in relation to CI during human-made and natural disasters. As such, this paper provides new insight into CI resilience by examining public expectations of CI operators during and after disasters. It does so by drawing on key themes that emerged from a review of the literature on public expectations of CI and presenting results from an online questionnaire-based study (N=403) of disaster-vulnerable communities in France, Norway, Portugal and Sweden. Regarding the minimum acceptable level of service and recovery time, questions were asked for two sectors: water and transportation. Respondents were asked about the acceptability of four below normal service levels for each sector and also about the amount of time they would be willing to tolerate said disruption (from ”years” to ”not at all”). The paper provides empirical evidence that suggests that the public are willing to tolerate reductions in the level of service. When it comes to duration, the public appear willing to tolerate a reduction for either ”weeks” or ”days,” or ”weeks” or ”months”. The willingness to tolerate a disruption seems to be linked to the amount of inconvenience a given disruption would inpart. This suggests that the expectation gap in terms of service provision may not be as wide as was found in the literature review, especially considering that information provision has been found to lead to more reasonable expectations [5]. As such, once known, the public's expectations and tolerance levels can indeed be used to establish targets for the implementation of resilience by CI operators. Acknowledgements: The IMPROVER project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653390.

Melkunaite, L. et al. (2016). International Survey. IMPROVER Project, Deliverable 1.1.

Barker, B. (2013). New Focus for Weathering Storms: Customer Resilience. In EPRI Journal.

Buller, A. (2015). Closing the Gap: Expectations versus Capabilities. In PA Times.

Iannucci, B. et al. (2013). A Survivable Social Network. In Technologies for Homeland Security (HST), 2013 IEEE International Conference on.

Bylund E, Lille J. (1999). Consumers perception of the Gothenburg Water utility business (In Swedish). Bylund & Lille AB, Stockholm.

CONTRIBUTION OF LOCAL GOVERNMENT TO DISASTER RESILIENCE: TOWARD AN ASSESSMENT METHOD

Eric Rigaud[1]

[1] MINES ParisTech, PSL Research University, CRC, Centre de recherche sur les risques et les crises (CRC) – MINES ParisTech - Ecole nationale supérieure des mines de Paris – CS 10207 rue Claude Daunesse 06904 Sophia Antipolis Cedex, France, France

Despite floods, sacking, shaking, burning, bombing, irradiation or poisoning most of the cities of the world have survived and are still existing [1]. During centuries, cities were, on the one hand, the symbol of protection for people living inside, symbol of order and rationality with police, administration, rules and justice as symbol of control over nature. On the other hand, cities have to cope with specific hazards such as fires, famines, epidemics and natural hazards such as earthquakes or volcanic eruptions [2]. The industrialisation led to the disappearance of famines and most epidemics and man-made risks such as fires are nowadays considered as accidents and no more as disasters. Nevertheless, industrialisation caused the emergence of megacities and consequently increased the interconnectivity between industrial systems, which led to the emergence of new types of disasters such as systemic risks. Resilience appears as a new paradigm for disaster management, with new expectations such as considering potential systemic or global risks, extending the scope of disaster management stakeholders including citizens and civil societies, increase capacities to respond to unforeseen situations, etc. In this document, definition of resilience provided by UNISDR will be used as reference: The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions [3]

Improvement of cities disaster resilience requires the interaction between two approaches. The first is a top down approach, according to which governments are expected to design proper disaster resilience mechanisms such as regulation and inspection regimes, and assign tasks to each level of responsibility. The second follows a bottom up approach, where local governments, citizens, communities, business, non-profit organisations share tasks to increase their risks culture and capacities to prevent, respond and recover from their occurrence [4]

This paper aims describing activities dedicated to the development of a methodological guideline aiming at assessing and enhancing the performance of local governments in the context of disaster resilience, which is easy to handle and applicable by all types of cities. The proposed methodology aims at representing the diversity of works and projects conducted in the context of city resilience to disasters by integrating different methods developed throughout Europe, the United States, Australia and New Zealand into one integrated approach. The paper is structured into three main sections. The first section is dedicated to the description of the resilience of cities towards disasters and to the role of local governments within disaster management. The second section outlines the results of the analysis of existing tools for resilience assessment for cities. The last section presents the first version of the solution for supporting the management of the contribution of local government to societal resilience to disasters and first lessons of its experiment.

Keywords: Disaster resilience, local government, assessment method

Oral Presentations

Resilience in Power Systems

SOCIOTECHNICAL NETWORKS FOR POWER GRID RESILIENCE: SOUTH KOREAN CASE STUDY

Daniel Eisenberg1, Jeryang Park 2, Thomas Seager 3

[1] Arizona State University, USA (ASU) – United States

[2] Hongik University – South Korea

[3] Arizona State University - ASU (USA) – United States

daeisenb@asu.edu

Despite broad engineering efforts to make power grids resilient to all hazards, maladaptive blackout response practices continue to exacerbate isolated failures into systemic losses. Power grid resilience understood by engineering experts focuses on designing robust infrastructure systems to reduce the probability that customers will lose access to electricity. In contrast, blackout response is organized by public administration experts focused on system rebound via policy and protocols to coordinate crisis response to unforeseen infrastructure losses. Together, robustness and rebound practices do not produce resilient power grids, as the large-scale, cascading power failures that overwhelm automatic controls and security constrained operations also overwhelm bureaucratic processes for information-sharing and decision-making established before the crisis. In fact, engineering and public administration approaches to resilience are often established absent from each other – the physical limitations of electric power transmission are not considered in response protocols and crisis management roles are not reflected in robust design. We argue that these isolated practices will continue to produce brittle infrastructure systems, and that blackout response must advance beyond robustness and rebound towards sociotechnical concepts that integrate infrastructure design and crisis management together. This work uses network science to measure how misconceptions of built infrastructure and their management systems influence sociotechnical resilience[i] in power systems. Network science has emerged in both power engineering and public administration disciplines as an important tool for identifying critical infrastructures that cause emergencies when failed and human interactions that dictate emergency response. We believe that the similarities in modelling and analysis across both disciplines signify the potential for corresponding social and infrastructure networks to mutually inform one another. Specifically, corresponding networks can reveal the mismatches between engineering design and public administration that cause maladaptive blackout response by quantifying: (1) biases in identification of critical infrastructures for failure protection activities, (2) the disconnect between organizational authority in normal operations and coordinated crisis response settings, and (3) which organizations may be more impacted by cascading failures. In this work, we study these three blackout response issues in the South Korean power grid. Network analysis is accomplished by developing corresponding infrastructure and social networks, applying statistical methods to reconcile conflicting interpretations of network models, and generating social networks associated with cascading infrastructure losses. Results demonstrate that separate understandings of engineered infrastructure and organizational coordination do not match those in sociotechnical practice – regions with few power grid infrastructures contain those most critical to grid protection, organizations with the most decision-making authority do not broker crisis management information, and few organizations are more adversely affected by cascades than others.

[i] Woods, D. (2015), Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety 141: pp.5-9.

Keywords: Electric Power Systems, Critical Infrastructure, Network Science, Sociotechnical, South Kore

RESILIENCE ACTIVATION AND LIMINALITY DURING THE FUKUSHIMA DAI ICHI NUCLEAR POWER PLANT ACCIDENT

Cécile Geoffroy [1], Eric Rigaud [1], Franck Guarnieri [1]

[1] Centre de recherche sur les Risques et les Crises (CRC) – MINES ParisTech - ´Ecole nationale sup´erieure des mines de Paris – Rue Claude Daunesse B.P. 207 06904 Sophia-Antipolis Cedex, France

This article will focus on the definition of the model of resilience activation (Powley 2009) and more specifically on the phase of liminal suspension. The goal is to test this model and to evaluate its contributions and limits. The testimony of Masao Yoshida, the manager of the Fukushima Dai Ichi nuclear power plant during the accident, that was held during official hearings on July and August 2011 (Guarnieri et al. 2015) will be used to test the model and achieve our goal of evaluation. According to Edward Powley (Powley 2009), resilience activates when organizations confront threats, challenges, or unexpected emergency situations. It defines an organization power to resume, rebound, bounce back, or positively adjust to untoward events. In order to understand this process and how individuals and collective are able to overcome the trauma caused by a crisis in their organization Powley presented a three-phase model. The Resilience Activation model (Powley 2009) considers that three key moments are necessary for an organisation to overcome a trauma: liminal suspension aims to restore the psychological, emotional and relational balance of all of the actors in the system, compassionate witnessing aims to restore social order and relational redundancy aims to restore the balance between the organisation and its environment. About this model we paid specific attention to the first phase: liminal suspension and, more broadly, liminality. In Powley's work (Powley 2004; Powley and Piderit 2008; Powley and Cameron 2008; Powley 2009; Powley 2013), liminality deals with the unknown, death, transition to a new life. This step is characterized by ambiguity, fear, danger and risk. Nor ranks nor status exist anymore. Individuals have to transform towards a new identity and new norms of relations in order to reconstruct themselves. Liminality is situated between two statuses; it is a moment of renewal that introduces change. The first section of the article will be dedicated to the presentation of the concept of resilience activation and of the liminal suspension phase as Edward Powley defined them, and to their confrontation with Resilience Engineering concepts and models. The second section will propose an illustration based on the study of Masao Yoshida's testimonies related to events that occurred within the Fukushima Dai Ichi nuclear power plant from 11th to 15th March 2011.

Keywords: Resilience activation, Liminality, Fukushima Dai Ichi

SUPPLEMENTATION OF THE RISK ANALYSIS OF fiRE IN THE MAIN TRANSFORMERS OF THE ITAIPU BINACIONAL HYDROELECTRIC POWER PLANT WITH RESILIENCE ENGINEERING ELEMENTS

Juliano Portela[1], Lia Guimaraes[2]

[1] Itaipu Binacional – Av Tancredo Neves, 6731 - Foz do Iguacu, Parana, Brazil

[2] Universidade Federal do Rio Grande do Sul - UFRGS (BRAZIL) – Brazil

jportela@itaipu.gov.br, liabmg@gmail.com

Serious accidents in critical infrastructures, although rare, cause significant social and economic impacts in their area of influence. The Itaipu Binacional Hydroelectric Power Plant, an organization with such characteristics, must avoid accidents throughout its operational cycle, even if a ”normal” accident rate is expected due to the high risk factors and complexity inherent to its operation. In order to succeed in avoiding them, a line of study considers important an evolution in safety management: formerly reactive, based on the retrospective analysis of accidents and ”what goes wrong”, now proactive according to Resilience Engineering (RE), which is based on the variability of normal operation and therefore ”what goes right”. By this approach, this article aims to propose a method to supplement the traditional risk analysis of fire in one of the main installation power transformers with elements of ER, by inserting proactive elements based on the experience of the team in a risk analysis based on the statistical failure analysis. It is justified by the socio-technical importance of the installation, by the constant technological changes and by a process of technological upgrading of all control, supervision and monitoring systems of its generating units and substations, making essential a proactive approach of operational safety of the plant. Considering the structured opinions of the operational staff and the precepts, techniques and heuristics of RE, indicators and action plans were proposed to increase the operational safety of regular work.

Keywords: operational safety, power plant, risk analysis

MODELLING ORGANIZATIONAL LEARNING FROM SUCCESSES IN THE NUCLEAR INDUSTRY

Kaupo Viitanen[1], Christer Axelsson [2], Ann Britt Skjerve [3], Hanna Koskinen [1], Rossella Bisio [3], Marja Liinasuo [1]

[1] VTT Technical Research Centre of Finland – Finland

[2] Vattenfall AB – Sweden

[3] Institute for Energy Technology – Norway

During the past decade there has been a growing interest in utilizing lessons learned from successful experiences to ensure safety in high-risk organizations. For example, the Safety-II approach to safety management emphasizes the understanding of how things go right. In our ongoing study we aim to provide insights into how successes can be identified and utilized for learning purposes in the nuclear industry. We conducted a literature review into the concept of learning from success and two empirical case studies at Nordic nuclear power plants to identify successes, lessons learned, and the learning practices utilized. Data collection consisted of interviews, document analyses of event reports and field observations. Drawing insights from existing theories, we modelled the findings from our study from the perspective of organizational learning and knowledge management. The purpose of this exercise was to understand how learning processes are utilized in the context of successes in a high-risk organization, what special considerations might be necessary to take into account when facilitating organization learning from successes and what practical tools exist that can support this effort.

We identified four learning-related phases from our data. The first phase – identification and acquisition – serves as the starting point for a learning agent. Within our study, we found three types of means through which success-related information can be acquired: identification of own successful decisions and actions; actively retrieving success-related information by asking from colleagues, reading reports, analysing databases, or conducting investigations; and receiving success-related information through listening to storytelling or participating in trainings. The second phase relates to creation of the lesson. Characteristic activities of this phase are, for example, providing a salient starting point and structure for analysis or reflection, encouraging finding positive aspects within adverse situations and ensuring that the right lessons are learned in order to avoid confirming risky habits or creating organizational drift. The third phase is about storing the success-related knowledge. Storage can take many forms: it can be explicitly codified in systems, or tacitly embedded in individuals or culture. The stored knowledge can then be, in the fourth phase, either utilized in practice or communicated actively to others. The existence of easily accessible communication channels is of relevance in ensuring the effectiveness of active communication of success-related knowledge. In this paper we will describe the results of this modelling exercise in further detail and provide examples of practices that may facilitate learning from successes in each of the phases based on our observations from the empirical case studies. In addition, we will present generic types of information flows that illustrate the routes along which success-related information (e.g. lessons learned) may get passed in the organization. This can help pinpoint the processes and practices that facilitate organizational learning from successes. Finally, we will discuss how such a modelling exercise can benefit practitioners working in high-risk industries aiming to develop their organizations so as to learn more effectively and systematically from successful experiences.

Keywords: organizational learning, learning from successes, knowledge management, nuclear industry

RESILIENT POWER PLANT OPERATIONS THROUGH A SELF-EVALUATION METHOD

Mikael Wahlström ∗ 1, Timo Kuula 1, Laura Seppa¨nen 2

1 VTT Technical Research Centre of Finland (VTT) – Vuorimiehentie 5, FI-02150, Espoo, Finland, Finland 2 The Finnish Institute of Occupational Health (FIOH) – P.O. Box 40, 00251 Helsinki, Finland, Finland

An important aspect in system resilience is the quality of work practices. Assumedly, in nuclear power plant operations, being able to consider situations interpretatively provides good basis for handling various kinds of challenges, that is, with consideration to various information sources and with profound understanding of the plant dynamics as well as in dialogue within the operator crews [1]. This implies that developing training for developing work practices could enhance system resilience. Certain challenges have been identified in the existing training practices at a specific Nordic power plant site: the crews would need opportunities to witness and exchange the practices with the operators of other crews for the proliferation of good practices between the work shifts. The current safety procedures also dictate operator activity very specifically – capability to handle new kinds of situations is not therefore efficiently developed in the emergency training where these procedures are applied. Exchange and creation of good work practices along with opportunities for more 'freeform' simulator try-outs for more profound understanding of the plant dynamics would be beneficial. Some of the challenges might reflect the nuclear domain's safety critical and hierarchical nature – generally, transition from training where learners are 'passive objects' to 'active and critical subjects' would be necessary [2]. For enhancing simulator training, we generated a self-evaluation method that aims to disseminate good practices by the means of guided dialogue among the operators. It consists of 1) personal evaluation, 2) group evaluation and 3) inter-group learning. The data collected for this study represents the first two phases. Two questionnaires were constructed for evaluation in first two phases, including simulator task performance related open-ended questions and statements with rating scales. The group discussions (phase 2) were recorded for data collection and analysis. The focus of analysis is on operator crews' reflections on the simulator tasks. In short, reflection here means talk where the operators are analysing or commenting on themes prompted by their simulation experience or by the self-evaluation guideline. Reflection is expressed as uncertainty or doubt, dilemmatic speech, expressions of challenges, evaluation or questioning, and expressions of feelings [3]. As a preliminary result, reflection was quite abundant in the broad sense, consisting of more than a half of all discussion. In this sense, we could say that self-evaluations were efficient in enhancing operators' reflection: they involved dialogue and reflection among operator crews about their own work practices and capability in emergency situations. However, it is not certain how these contribute to the interpretativeness in actual work practices.

Savioja, P., Norros, L., Salo, L., & Aaltonen, I. (2014). Identifying resilience in proceduralised accident management activity of NPP operating crews. Safety Science. 68: 258–274.

Wahlström, M. & Kuula, T. (2016). Organizational self-determination and new digital selfstudy applications as means for developing nuclear power plant operation training. Proceedings of HCI International 2016 conference, Toronto, Canada, 17–22 July, 2016 (pp. 650-660).

Heikkilä, H. & Seppanen, L. (2014). Examining developmental dialogue. The emergence of participants' transformative agency. Outlines. Critical Practice Studies, 15(2), (pp. 5-30).

Keywords: resilience, training, nuclear power plant operations, work practices

Oral Presentation

Assessing Resilience

FRAM TO ASSESS PERFORMANCE VARIABILITY IN EVERYDAY WORK: FUNCTIONAL RESONANCE IN THE RAILWAY DOMAIN

Riccardo Patriarca[1], Giulio Di Gravio [1], Francesco Costantino [1], Massimo Tronci [1]

[1] Department of Mechanical and Aerospace Engineering - Sapienza University of Rome (Sapienza DIMA) – Via Eudossiana 18 - 00184 Rome, Italy

riccardo.patriarca@uniroma1.it

Modern trends in the field of safety analysis of current socio-technical systems suggest developing an integrated view on technological, human and organizational aspects of the system. The traditional safety assessment techniques might become ineffective, since they generally evaluate only linear causal dependencies, based on the principle of decomposition, failing at identifying transient and dynamic interdependencies. The Functional Resonance Analysis Method (FRAM) aims to fill this gap, as proved by several FRAM applications in different industries and organizations, even at different operational levels. FRAM aims to define complex systems looking at their functional aspects rather than their physical structure. Therefore, it shows how systems actually perform in everyday work, adapting their functioning to deal with the variability of current operating conditions.

This paper shows the possibility of enhancing the traditional FRAM structure by a semiquantitative framework in order to increase its applicability for the analysis of complex systems. This innovative framework consists of defining numeric scores for variability, quantifying in a particular scenario the effects of interactions among functions. In addition, rather than static and deterministic values, it assigns probability distribution functions to the scores, mixing them by the aid of Monte Carlo simulation. The distributions, based on Subject Matter Experts' judgments and historic data, if available, allow measuring variability of performance and subsequent effects in terms of critical functional resonance. This semi-quantitative framework allows isolating the critical functions and the critical links among functions, considering non-linear and transient interdependencies. Furthermore, this paper explores the possibility of combining the Monte Carlo framework with a framework based on different abstraction layers, to make more evident and readable the model itself, maintaining a systemic functional perspective. Once addressed the criticalities and related them to different levels (operational, tactical, strategical), it would be possible to decide the priority for future mitigating actions. The illustrative case study takes advantage of SMEs and several accident reports in the railway domain to analyze specific accident data, according to a resilience engineering perspective, clarifying the application of the proposed frameworks based on FRAM.

Keywords: Safety assessment, Resilience, Functional resonance, Monte Carlo, Abstraction, SME.

A STAMP BASED TASK AND ORGANIZATIONAL ANALYSIS TO IMPROVE AIRCRAFT GROUND HANDLING SAFETY

Mario Pierobon[1], Graham Braithwaite [2], Jim Nixon [2]

[1] Cranfield University – Cranfield Bedfordshire MK43 0AL United Kingdom, United Kingdom

[2] Cranfield University – United Kingdom

m.pierobon@cranfield.ac.uk

The research work proposed for presentation as a paper is an output of a research project investigating aircraft ground handling safety based upon the systems theoretic accident model and processes (STAMP)[i]. The work consists of (1) a task analysis of the aircraft ground handling process and (2) an analysis of the organizational setup of aircraft ground handling companies in support of the implementation of safety control actions in the aircraft ground handling environment. The task analysis (1) consists of a functional decomposition and was initiated by means of line observations following the various input-process-output (IPO) flows occurring in aircraft ground handling operations in order to functionally characterize the controlled process of aircraft ground handling to the highest level of detail (the third level of a functional hierarchy). Collected data were then reported in the functional flow block diagram (FFBD) format and clusters of functions determined at the second level of the functional hierarchy; the latter were then further clustered together to determine the first level of the functional hierarchy. Second and first level functions were also drawn in the FFBD format. The task analysis was continued with the identification of the safety control actions[ii] enforced over second level functions, as documented in the IATA Ground Operations Manual (IGOM). The task analysis was conducted with the aim of characterizing the aircraft ground handling process both horizontally - with respect to the informational transformations that occur through the several IPO flows - and vertically - with respect to the safety control actions that have to be implemented to maintain safe performance. The task analysis has led to a detailed horizontal and vertical characterization of the aircraft ground handling process and to an improved understanding of the differences between functions - the informational transformations that occur within a process - and safety control actions - the precautions or conditions that must be satisfied to perform a function safely.

The organizational analysis (2) is being conducted by means of an on-line survey distributed to aircraft ground handling operations managers and aiming to depict the consistency in the implementation of safety control actions and feedbacks at three control levels within aircraft ground handling companies: the corporate over operations management control level, the operations management over line employees control level, and the line employees over aircraft ground handling process control level[iii]&[iv].The survey is being complemented by twenty semi-structured interviews to aircraft ground handling operations managers; the interviews are focused on safety performance enablers and inhibitors, as well as on possible status quo improvements, across the three levels of control detailed above and within five control dimensions in aircraft ground handling companies: the quality system, the training system, the safety culture, the supervision system, and the operations design system. The interviews are being transcribed and are being coded for analysis based upon the control loop taxonomy of STAMP: controller (and related control action generation and system model); control action(s); controlled party; and feedback(s).

The control loop taxonomy of STAMP is being applied across the five different control dimensions and the three different levels of organisational control, and based on whether the themes refer to enablers or inhibitors of performance and whether they refer to the status quo or possible improvements. The organisational analysis has been undertaken with the aim of identifying regardless of any specific safety control action directly exercised over the aircraft ground handling process - both enablers and inhibitors of safety performance within the organisational setup of aircraft ground handling companies. The aim is also to identify possible (additional) improvements for organisational redesign based upon the STAMP model of accident causation. Early transcript coding exercises are allowing the deployment of the – generic – control loop taxonomy at three aforementioned levels of control and across the five aforementioned control dimensions; an aircraft ground handling specific taxonomy is also emerging from the transcript coding exercise that is linked to the generic taxonomy: a theme is coded with both the code pertaining to the applicable category of the control loop taxonomy and with a nominal phrase summarising the theme. As an example, the recurrent theme of IGOM's adoption by aircraft ground handling companies is considered as an enabler of safety performance (+) occurring within the operations design system (ODS) that classifies as a corporate over operations management (CO) control action (CA) representing the status quo (SQ) and therefore generically coded as +ODSCOCASQ. The same theme, however, is also being specifically coded as 'IGOM's adoption by corporate management'.

i Leveson, N. G. (2004). A new accident model for engineering safer systems. Safety Science, 42, 237-270.

ii Leveson, N. G. (2011). Engineering a Safer World - Systems Thinking applied to Safety. Cambridge, Massachusetts, USA: MIT Press.

iii Rasmussen, J., & Svedung, I. (2000). Proactive risk management in a dynamic society. Karlstad, Sweden: Swedish Rescue Services Agency

iv Leveson, N. G. (2004). A new accident model for engineering safer systems. Safety Science, 42, 237-270.

Keywords: STAMP, resilience, aircraft ground handling, safety, system safety

LESSONS FROM THE DESIGN OF A RESILIENCE ENGINEERING BASED SOCIO-TECHNICAL SYSTEM DIAGNOSTIC METHOD

Eric Rigaud[1]

[1] MINES ParisTech, PSL Research University, CRC, Centre de recherche sur les risques et les crises (CRC) – MINES ParisTech - Ecole nationale supérieure des mines de Paris – CS 10207 rue Claude Daunesse 06904 Sophia Antipolis Cedex, France, France

This paper aims contributing to the application of resilience concepts and precepts to the design of operational methods and tools with presenting and discussing lessons learned from a collaborative process involving researchers, railway experts and operational agents designing and experimenting a method for analyzing socio-technical system resilience performance. First part of the paper aims describing the key phases of the process followed. Starting from the Resilience Analysis Grid (Hollnagel 2013) two prototypes has been successively specified, designed and experimented. For each of these six phases, the context, the methodology and the results obtained will be presented and commented. Second part of the paper will be dedicated to the discussion of a set of lessons learned from this process. Lessons will be related to theoretical concepts, method scope, performance model, data collection and analysis and experiments.

Keywords: Resilience Analysis Method, Railway, Lessons learned

TRACKING THE EMERGENCE OF RESILIENCE: THE ROLE OF COMPLEXITY

Tarcisio Saurin[1], Guillermina Penaloza [1], Marlon Soliman [1], Carlos Formoso [1]

[1] Federal University of Rio Grande do Sul (UFRGS) – Brazil

saurin@ufrgs.br

Resilience in complex socio-technical systems (CSSs) takes a wide variety of forms – e.g. proactive, reactive, organizational, individual, team, etc. Nevertheless, little is known on the origins of resilience, which is usually regarded as an emergent phenomenon arising from dynamic interactions between several factors. While this "emergent" perspective is correct, it does not explain how fundamental system characteristics interact to generate resilience. In this paper, we discuss the role of complexity attributes in the emergence of resilience. We build on a previous work [1], which has proposed four categories of CSSs attributes: a large number of dynamically interacting elements, a wide diversity of elements, unexpected variability, and resilience. Figure 1 (see word file) presents a model of the interactions between the attributes. However, each of the four groups of attributes has a number of dimensions, thus making the relationships displayed in Figure 1 an oversimplification. For instance, diversity of skills of the workforce can interact with resilience in a very different way than technical diversity of materials and equipment. In order to go further in this analysis, we propose a framework (Table 1 - see word file) that shows how some dimensions of the CSSs attributes interact with the four potentials of resilience systems [2]: anticipation, monitoring, responding, and learning.

In this paper, we report an empirical test of some of the propositions implicit in Table 1. This test was carried out in a construction site, by: (i) applying a questionnaire to workers and managers, so as they could point out the extent to which complexity attributes were present; (ii) interviewing workers and managers, in order to spot perceptions about the construction site's complexity; (iii) describing the four sub-systems that form the socio-technical system under investigation (i.e. technical, social, work organization, and external environment); and (iv) conducting a resilience assessment, by using the Resilience Analysis Grid2(RAG). Data from (i), (ii) and (iii) were cross-checked with data from (iv), thus setting an empirical basis to discuss Table 1.

Righi, A.W., Saurin, T.A. 2015. Complex socio-technical systems: characterization and management guidelines. Applied Ergonomics 50: 19-30.

Hollnagel, E. 2015. RAG - Resilience Analysis Grid. Introduction to the Resilience Analysis Grid (RAG). Technical note available at < http://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf> . Accessed at October 31, 2016.

CAN ARTEFACTS BE ANALYSED AS AN AGENT BY ITSELF – YES OR NO: WHAT DOES HUTCHINS 'HOW DOES A COCKPIT REMEMBER ITS SPEEDS' TELL US

Anthony Smoker[1], Arie Adriaensen [2], Riccardo Patriarca[3], Johan Bbgstrom [2]

[1] Lunds Universitet, Division of Risk Management and Societal, Sweden (LTH) – Lund University Box 118 22100 LUND, Sweden

[2] Lunds Universitet, Division of Risk Management and Societal Safety, Sweden – Sweden

[3] Sapienza University of Rome, Department of Mechanical and Aerospace Engineering – Italy

anthony john.smoker@risk.lth.se

Hutchins' paper 'How a Cockpit Remembers Its Speeds' (Hutchins, 1991), emphasised the unit of analysis in exploring the processes and knowledge structures that underpin the activity of a socio-technical system. The context in which artefacts are situated is implicit to understanding socio-technical systems and their underlying processes. Analysts undertaking explorations of socio-technical systems are confronted with an analytical dilemma: where to begin to frame the exploration to derive appropriate and relevant questions to ask. One approach is to explore the interactions between system elements (sub-systems) that comprise flows of information or tasks within the work system.

Resilience engineering has an interest in the interactions between sub-systems. These dictate and influence the availability of sources of resilience that can be drawn upon in exploiting the systems adaptive capacity escalation in response to performance variability as well as the consequences upon other system elements.

Resilience engineering conceives these interactions through the work-system and strategies that are employed when deploying sources of resilience, reconfiguring & adapting the work system. Hutchins investigated this through conceiving the cockpit as a joint cognitive system: how a work-system observed and remembered the speeds by which the aircraft operated. In turning non-observable properties of system performance into adaptive strategies, Hutchins offers the RE community a potential way to study the work-system.

FRAM is proposed as a tool that provides the means by which a work-system can be explored taking system and functional perspectives of the work-system. It is acknowledged that FRAM has limitations. Some relate to the definition of the system of interest. Of more relevance is the question that the FRAM model is built to explore.

A FRAM study was undertaken of the Hutchins' 1991 work-system and three pilots who flew the DC9 provided the domain knowledge to produce an ecologically valid FRAM model through interpreting the documentation and procedures that shape the work system. The FRAM study modelled the joint cognitive system of the flight deck for the specific phase of flight that Hutchins examined – the descent phase, from top-of-descent to final approach.

It is widely recognised that developing an understanding of the work system is an essential preparatory stage. FRAM produces a view of how sources of resilience can be deployed with an assessment of their properties, but some other analytical mechanisms outwith FRAM are required to yield a structured approach

By using a structured approach, knowledge of the suitability of FRAM to explore a work system previously studied could be assessed, and the results compared. Especially, Hutchins' interest in exploring beyond mere human agents that can alter the focus on other units of analysis that might otherwise be overlooked. FRAM analysis might not need some of these emergent units of analysis and could describe performance variability without these additional constructs.

The paper will report what was undertaken, the understanding gained and results drawn with a comparison made with Hutchins paper and usefulness and utility of specific preparatory steps before building a multi-layered FRAM model.

Keywords: RE, Sources of resilience, FRAM, socio, technical systems, work system, cognitive artefacts, Joint cognitive systems, system properties

METHODS AND ANALYTICAL FRAMEWORKS FOR EXPLORING ADAPTIVE CAPACITY

Anthony Smoker[1], Matthieu Branlat [2], Ivonne Herrera [3], Rogier Woljter [4], Billy Josefsson [5]

[1] Lunds Universitet, Division of Risk Management and Societal, Sweden (LTH) – Lund University Box 118 22100 LUND, Sweden

[2] SINTEF (SINTEF) – Norway

[3] SINTEF – Norway 4 FOI – Sweden 5 LFV – Sweden

anthonyjohn.smoker@risk.lth.se, matthieu.branlat@sintef.no

As the interest in Resilience engineering grows, so does the need to have operationally viable methods that can be applied to provide meaningful assessments of resilient performance. A methodology that is accessible to a community of practitioners that are unlikely to have extensive background theoretical knowledge of the concepts of Resilience Engineering is sought. In two SESAR Projects, development of a methodology to assess resilient performance as part of a larger safety assessment method was undertaken iteratively. The resulting RE method was integrated into the Safety Reference Material, it being mandatory in the SESAR safety assessment methodology to assess whether a project will benefit from an R.E. assessment of the designs used in SESAR operational concept development projects that exploit the potential of new technologies.

Taking the earlier derived RE method, it was applied on two new operational concepts for further development. Following the first of these applications, a critical review led to recognition that derived RE method required further development with a change of emphasis.

In order to understand adaptation and resilient performance in work systems, which was the objective of the assessment methodology, it was decided to use an understanding of the strategies that are enacted as work-as-done that are employed in managing and responding to surprises and the underlying philosophy of the adaptation. This focus required that the potential features of the operation, the sources of resilience and resources drawn upon, the way in which escalation can take place, the trade-offs that are faced and the means by which the work system can return to some stable state were understood. The consequences of these adaptations are elicited therefore, from the knowledge of those who undertake the work in real world settings.

The methods and techniques to understand resilient performance - by exploring the adaptive properties of the work system and its associated consequences - were explored and a methodological framework developed. The methodology was developed from critically reviewing available methods, selecting those to use drawn from systems thinking techniques, knowledge elicitation and other methods that provide the means to carry out meta-analysis. These were then applied on three new concepts for ATM system development, in an analytical framework including several methods that have been employed in studies of resilience, and some that had not.

The RE assessment methodology evolved into an analytical strategy that was subsequently used by domain safety practitioners, who operationalised the methodology.

A step by step process evolved that included building an understanding of the work system in preparation for a workshop; the output being captured as visualisation of the current and proposed work system. This formed the basis for an eventual functional synthesis of both current and envisaged work systems. A workshop was used as the principal means for exploring resilient performance of the current operation and the future design. This paper discusses and reports the evolution of the RE assessment methodology, critically reviews the methods employed, the analytical strategy derived and discusses the results achieved

Keywords: Adaptive Capacity, RE, Methodology, methods, adaptation, graceful extensibility, work, as, done, work system, RE assessment methodology

Oral Presentations

Organizing Team Resilience

SAFE MOORING OPERATIONS: A FUNCTIONAL APPROACH TO ROUTINE WORK?

Nippin Anand [1]

[1] Safety Management System, DNV GL - Maritime – Netherlands

nippin.anand@nippinanand.com

This paper is an enquiry into mooring of merchant vessels. Much can be learnt by understanding routine work rather than analyzing an accident as an isolated event to the depth of details. The severity of an isolated accident tells us much less about how a system functions than frequent undertaking of routine work except that in the case of latter we lack a vocabulary and method. Unfortunately, this is how we understand most accidents and hence fall into a negative framework of shaming and blaming the people and 'fixing' the system. What follow is more controls, procedures and barriers none of this of much practical value if we fail to understand how routine work is performed. This paper introduces a method and a vocabulary to make sense of routine work through firsthand experience of an accident of the author.

FROM RESILIENCE TO ROUTINES AND BACK: INVESTIGATING THE EVOLUTION OF WORK ADAPTATIONS

Jop Havinga [1], Sidney Dekker [2], Andrew Rae [2]

[1] Griffith University – Safety Science Innovation Lab Macrossan Building N16 Room 2.22 170 Kessels Road Nathan, QLD 4111, Australia

[2] Griffith University – Australia

SIGNIFICANCE PROBLEM: No socio-technical system is fully pre-specified: people always fill in gaps. This is a sign of resilience: the ability to adapt to changing circumstances to meet production and safety expectations. However, when teams do the same task multiple times, teams do not only respond to their current conditions. Teams also replicate parts of what they have done before; they also have a path dependency. Our research has explored the space between variation and replication in performing a task, the formation of a routine, and the change of routines.

METHOD: To investigate this, we studied both blast crews in mines and power line crews. Both blast crews and power line crews do safety critical work and have (partly) interchangeable roles within crews. We conducted fieldwork for a total of seven weeks (usually with 12-hour shifts) across different crews and different locations. The fieldwork consisted of observation, as well as semi-structured interviews about what people would do in different situations. The focus was on: • How different actions followed each other • Differences and similarities between different instances of similar tasks • Differences and similarities within crews, between crews and between locations • Historical changes in how people would have addressed similar problems

RESULTS SO FAR: While the literature often described routines as repeating patterns of actions, we found considerable variation in the patterns of actions. However, we did find consistency in 'in-between-states' towards the completion of the goals and meaning given to the environment. Practitioners used different actions, different orders of actions, and different resources the reach the same state. The idea that there was an ideal pattern of actions did not fit, instead, crewmembers acted opportunistic by using what was available. For some isolated tasks, some crew members in one crew could show certain patterns more often than other crew members did, but crew members were not aware of these differences nor did these differences have any noticeable effect. However, crewmembers would correct each other on differences in in-between-states created, even if the created states were functionally as good. The standardisation of in-between-states created recognisable markers of task progress and made incidental deviations stand out. The standardisation also allowed for team 'cultures' to form, where crews had their own symbols and associated meaning. While there is replication in routines, routines are not completely permanent. Routines can evolve quickly, even without crewmembers explicitly instructing each other. One change often creates the conditions for the next change. Elements that facilitated change included; goal feedback, varying task conditions, exchanges of practitioners between crews, and a semiotic system that supports coordination of new goals and constraints. CONCLUSION The actions of a team can quickly change if the environment changes. However, there was consistency in the problem understanding, a division of the problem space into sub-goals, and the semiotic system. To these sub-goals, there is freedom how these are reached. These elements are carried over through between enactments and show permanence between enactments but can change over time.

Keywords: routines, long term adaptation, team resilience, semiotics

IMPROVING TEAM RESILIENCE BY SUPPORTING MINDFUL COOPERATION AWARENESS

Christian Kunz [1], Nina Saric [1], Katrin Fischer [1], Toni Wäfler [1]

[1] University of Applied Sciences and Arts Northwestern Switzerland - School of Applied Psychology (FHNW) – Riggenbachstrasse 16 CH-4600 Olten, Switzerland

christian.kunz@fhnw.ch

Background Resilient teams are able to adapt to dynamic working conditions (Rankin, Lundberg & Woltjer, 2014). This ability emerges from cooperation of team members. When the same people work together over a longer time period, team specific patterns of cooperation evolve, triggering mutual expectations among team members. These patterns and related expectations reflect cooperative adaptations to dynamic working conditions. They foster team resilience and are a part of a teams' collective (embedded, see Lam, 2000) tacit knowledge.

Collective tacit knowledge evolves from the cooperation of different team members and hence from the interaction of different individuals' tacit knowledge. Such, it incorporates individual tacit knowledge regarding local adaptation strategies, which has (unconsciously) settled in over time. Sometimes these strategies do not entirely comply with official guidelines.

Over time, team members individually and often unconsciously develop expectations regarding the cooperation within the team. These expectations as well as their mutual compatibility are key elements of both, of the collective tacit knowledge as well as of distributed situation awareness (Salmon et al., 2009). A lack of systematic cultivation of such collective tacit knowledge may cause disruptions in cooperation, e.g. in case of staff fluctuation. New team members unfamiliar with the team specific cooperation patterns may base their actions on official guidelines and standards while, at the same time, long-time team members behave according to the patterns that settled in over time. This can lead to an incompatibility in mutual expectations causing disruptions in cooperation and finally reducing team resilience.

Developed and pilot tested method :

In close cooperation with Swiss NPP's a method was developed and piloted that supports systematic cultivation of collective tacit knowledge. The method supports the elicitation (Nonaka & Takeuchi, 1995), the sharing and the cooperative handling of collective tacit knowledge as well as of potential uncertainties emerging from incompatible mutual expectations. Such, the team members' cooperation awareness is enhanced, incompatible expectations are revealed and disruptions in cooperation can be prevented.

The method incorporates three parts: a pre-job workshop, a post-job workshop and a systematic exchange of tacit knowledge and mutual expectations during job execution. The three parts build on one another supporting stepwise deepening mindful cooperation awareness.

Result of pilot test :

The pilot showed that the systematic fostering of cooperation awareness enables an ongoing monitoring of mutual expectations and uncertainties regarding cooperation thereby making explicit individual as well as collective tacit knowledge. Such, incompatibility in mutual expectations can be anticipated earlier and proactive measures can be taken to avoid disruptions in cooperation. Furthermore, team members become more mindful regarding success-relevant aspects in cooperation which normally are often not taken into account. Thereby they are also empowered to recognize conflicts between being resilient and ensuring compliance in the cooperation at an early stage. Furthermore, a regular application of the method supports an organization to learn from tacit knowledge based local adaptations. The method as well as the results of the pilot will be presented in detail in the paper.

Keywords: team resilience, collective tacit knowledge, cooperations awareness, mindfulness, mutual expectations, local adaptations

PREPARING TO BE UNPREPARED: TRAINING FOR RESILIENCE

David Passenier[1], Daan Pool[2], Amy Rankin[3], Alexei Sharpanskykh [2]

[1] Department of Organization Sciences - VU Amsterdam – Netherlands

[2] Aerospace Engineering - Delft University of Technology – Netherlands

[3] Department of Computer and Information Science - Link¨oping University – SE-581 83 LINKOPING SWEDEN, Sweden

d.m.pool@tudelft.nl, amy.rankin@liu.se, o.a.sharpanskykh@tudelft.nl

Practical knowledge and experience are increasingly regarded as crucial facets of operational resilience. Resilience matters in conditions where people work under high pressure in dynamic and unpredictable settings, facing major consequences if something goes wrong. People working in such conditions build knowledge and experience by learning in formal training, participating in communities of practice, and internalizing lessons from on-the-job performance. Knowledge and experience thus gained can make people resourceful and enable them to act adequately in surprising and ambiguous situations. Formal training provides important building blocks to operate resiliently but can also obstruct resilience when instructions are only about following procedures. Procedures are useful guidelines in ambiguous, complex situations when operators know when, how, and why to deviate. This raises questions about what training for resilience would look like. How could such training access and stimulate experiential learning and informally acquired knowledge? For what kind of situations could or should operational personnel be prepared to deviate-emergencies, routine situations, or both? Could or should formal training simulate the real world better? In this paper we formulate a research agenda to develop useful theoretical insights about training for resilience. We draw from our diverse research experiences to outline topics of interests, methodological challenges, and contributions to practice.

1) Flexible vs robust procedures. How can operators be guided to know when to deviate from normal procedure?

Research in aviation suggests that a negative connotation with deviance is problematic in training for resilience. Deviating from procedures is generally seen as potentially dangerous, 'deviant' behavior. It can be hard to discuss operational practices outside this normative risk and safety management discourse. Ethnographic research, however, suggests that deviating is often routine, normal, and necessary to manage emergent risks on an everyday basis. To understand how, when and why deviating can be normal and not inherently dangerous is a major theoretical topic of interest.

2) Training general problem skills. Can general problem-solving skills provide a useful baseline to adapt to unexpected events?

In many disciplines, simulator-based training plays an important role in facilitating resilience. Non-normal and hazardous scenarios are increasingly trained in simulators, but it is difficult to match the surprise factor inherent in many critical and unexpected events. One way of enhancing the generalizability of trained skills is through scenario-based training. Another promising, yet underexplored, approach is the use of augmented-reality techniques to artificially enhance awareness of task-specific constraints during training and support higher-level learning.

3) Develop training programs based on knowledge of "work-as-done". How can knowledge about everyday challenges and adaptive performance inform training scenarios? Gathering and interpreting evidence to make informed decisions about training needs currently relies on models that largely exclude complex socio-cultural dynamics. Such models have, for example, difficulties explaining how workarounds emerge from interactions within a community of practice. A promising approach to modelling emergence of systemic properties in complex sociotechnical systems is agent-based modelling and simulation. A major challenge in this approach is integrating social scientific theories with computational agent-based models to understand and improve resilience.

Keywords: surprise, deviance, simulator training, augmented, reality techniques, agent, based modelling and simulation.

INNOVATION RESILIENCE BEHAVIOUR IN TEAM WORK

Peter Oeij [1]

[1] TNO [Pays-Bas] – Schipholweg 77-89, 2316 ZL Leiden, Netherlands

In this paper the focus is on the sustainability of people at work. This means that workers need to remain healthy, employable and vital and resilient (have the ability to bounce back from adversity). Remaining healthy, employable and vital, asks for human resilience at work or for workers' ability to bounce back from adversity (Demerouti, Bakker, Nachreiner & Schaufeli; Hobfoll, 2011; Salanova, Schaufeli, Xanthopoulou, Bakker, 2010). This contribution is projecting that starting point on teams and on a specific type of work, namely carrying out innovation projects. There is much debate about the failure of innovation and of projects. We explore what team environment can help to reduce such failures, and whether such environments – that we call mindful infrastructures – enable teams to be more effective and successful. For this purpose we look at teams from other context, namely teams of High Reliability Organisations (HROs). HROs deal with high risks but hardly ever fail. Such organisations – like nuclear plants, aircraft carriers, fire brigades and surgical operation rooms – develop highly reliable team behaviours, which they label as 'mindful' and 'resilient' (Weick & Sutcliffe, 2007). We transfer this kind of team behaviour to the context of innovation management and brand it as 'innovation resilience behaviour', the ability to bounce back from critical incidents that may cause innovation projects to fail, and to ensure the team stays on track to achieve its project goal (Oeij, Dhondt, Gaspersz & de Vroome, 2016). Can innovation teams benefit from the experience of HRO-teams? Literature:

Demerouti, E., Bakker, A.B., Nachreiner, F. & Schaufeli, W. B. (2001). The job demandsresources model of burnout. Journal of Applied Psychology, 86, 499-512.

Oeij, P.R.A., Dhondt, S., Gaspersz, J.B.R. & De Vroome, E.M.M. (2016). Can teams benefit from using a mindful infrastructure when defensive behaviour threatens complex innovation projects? International Journal of Project Organisation and Management, 8(3), 241-258.

Salanova, M.; Schaufeli, W. B.; Xanthopoulou, D.; Bakker, A. B. (2010). The gain spiral of resources and work engagement: Sustaining a positive worklife. In A. B. Bakker (Ed.), Work engagement: A handbook of essential theory and research (pp. 118-131). New York (US): Psychology Press. -Weick, K.E. & Sutcliffe, K.M. (2007). Managing the unexpected. Resilient performance in an age of uncertainty (2nd ed.; 1st ed. 2001). San Francisco: Jossey-Bass.

Keywords: reslience, teams, innovation, mindful organising, project

OPPORTUNITIES FOR SYNERGIES BETWEEN RESILIENCE AND A POSITIVE WORK ORGANISATION

Gerard Zwetsloot[1,2]

[1] Gerard wetsloot Research Consultancy (GZ RC) – Linnaeushof 64, 1098 KP Amsterdam, Netherlands

[2] Nottingham University – United Kingdom

Opportunities for synergies between Resilience and a positive Work Organisation. Twenty-seven companies in seven European countries participated in a research on the implementation of the Zero Accident Vision (Zwetsloot et al 2015). Though most of these companies explored several innovative ways to improve safety, none of the 27 companies explicitly referred to the concepts of resilience engineering or high reliability. In a survey it was confirmed that there was still a clear opportunity to further improve in this area.

Nevertheless, these ZAV companies seem to develop their organisational capacities in the direction of more resilient companies, which enjoy higher reliability. They developed their capabilities for monitoring, anticipation, and learning, (known to be relevant for resilience, (Hollnagel et al. 2006 and Hollnagel 2011). There was a high 'individual commitment to zero' from managers and workers, they developed the alertness to hazards and risks, and scored high on 'safety empowerment'. In some companies the people were 'invited to challenge their supervisors'. These capabilities seem to be aligned with respectively preoccupation with failure, sensitivity to operations, deference to expertise, and reluctance to simplify (capabilities know to be important for High Reliability Organisations, Weick & Sutcliffe 2007).

Several companies adopted the broader Zero Harm perspective, while most others recognised it is a future challenge to broaden their preventive efforts towards Health and/or Wellbeing at work. This will stimulate them to address the work organisation.

In resilience engineering deviations in processes are regarded as normal. In the research on work organisation and wellbeing at work where deviations are called 'demands' the worker has to deal with, that is also the case. Therefore, there seems to be plenty of opportunities for synergies between resilience, the implementation of a broad Zero Harm concept, and the promotion of wellbeing at work.

Goldenhar, Williams and Swanson (2003) showed a correlation between several work organisation factors (e.g. job demands, job control, job uncertainty, training, exposure hours, and job tenure) and safe work practices in construction, and Glasscock et al. (2006) found similar results in farming. Bergh et al (2014) found a correlation between psychosocial risk factors and hydrocarbon leaks on offshore platforms, whereas Ramvi (2003) showed a correlation between the quality of the psychosocial work environment and commitment to safety at work at two different oil installations in the North Sea. According to Chan (2011) fatigue is the most critical accident risk factor in oil and gas construction. A meta study by Nahrgang et al. (2010) showed that job demands and resources relate to safety outcomes.

Positive psychology (with its focus on 'resources') seems not only relevant for 'work engagement' but is also likely to be relevant for resilience and the safety 2 concept (Hollnagel 2014). Grøtan et al (2017) pay much attention to the role of 'resources' for increasing resilience capabilities. It is therefore important to explore synergies between resilience, reliability of production, and a positive work organisation, i.e. to include work organisation factors in the practices of resilience engineering.

Keywords: resilience capabilities, work organisation, wellbeing at work, positive psychology

Oral Presentations

Resilience Engineering, Definition, Moddeling & Methods

A PRACTICAL WORKSHOP-BASED METHOD FOR RESILIENCE ENGINEERING

Mariken Everdij [1], Sybert Stroeve [1]

[1] Netherlands Aerospace Centre (NLR) – Netherlands

Under the premise that a more resilient operation is better able to be safe and efficient, this paper presents a pragmatic approach for analysing the resilience of future air traffic management (ATM) operational concepts and improving their design. The approach uses a workshop with operational experts as a central element and follows 5 steps. The last two steps use key new elements specific for this approach; the first three steps are used in other safety methods as well, but are adapted to better support the last two steps. Step 0: Scoping - Planning and outlining the work to be undertaken.

Step 1: Describe operations - Building an initial understanding of the work-as-done in current ATM operations and of the way that future ATM operations are expected to be done.

Step 2: Varying conditions - Identifying a list of expected and unexpected varying conditions in the current and the future ATM operation.

Step 3: Adaptive capacity - Identifying the strategies that operators use when they are dealing with these varying conditions, and analysing the adaptive capacity of the current and future ATM operations. The strategies are acquired in a workshop session with air traffic controllers, pilots, supervisors and other experts. A narrative description of the available strategies, the decision-making process of when to use which strategy, the coordination required, the need to adapt each strategy to specific circumstances, and insight into how the strategy is acquired, i.e. through education or through practice and experience, provide input to understanding the resilience of the operation.

Step 4: Improve resilience - Deriving recommendations for strengthening the resilience of current and future ATM operations. In a workshop session, the operational experts involved in Step 3 identify improvements at the levels of design, management, operation and key performance areas such as safety, capacity, environment and cost-benefit. After the workshop, complementary design improvements are identified through analysis of all the material collected so far.

The approach is illustrated through application to an air traffic management (ATM) operational concept that uses Aircraft Surveillance Applications System (ASAS) for sequencing and merging of aircraft towards an airport. Output is an evaluation of the resilience of the operation, and the identification of a range of recommendations for the design of this operation, such that its resilience can be improved. This output has been used to further develop the ASAS sequencing and merging concept. The workshop sessions supporting Steps 1-4 have been designed to address all aspects of resilience, yet such that resilience engineering jargon is avoided as much as possible and the participants can express their views in close relation with their own operational experience. The operators in our workshop were very positive about the approach, which allowed them to explain all the things they do to make ATM safe, rather than getting blamed for some rare and difficult situations they were not able to completely solve given the circumstances. Resilience appears to be something they encounter in their everyday work.

Keywords: resilience engineering, method, workshop, air traffic management, future operations, practical, application

TOWARDS AN OPERATIONALIZEABLE DEfiNITION OF RESILIENCE

Samuel Huber [1], Thomas Kuhn [2]

[1] Forventis (Fv) – Wildbachstrasse 50 CH-8008 Zürich, Switzerland

[2] Armasuisse ST (ar) – Feuerwerkerstrasse 39 3602 Thun, Switzerland

Background: The concept of resilience is becoming widely used by many industries where safety and security is crucial for success. Often, resilience is being regarded as a homogenous concept, valid to be applied on individuals, organizations, government and even societies equally well. Unfortunately, this popularity led to rather diffuse definitions that are sometimes difficult to operationalize. In this paper, we present a definition of resilience that can be used in CD&E Experiments regarding socio-technical systems. Method: Principally, there are two different approaches to a definition of resilience. The typological (or deductive) approach is often referred to because of its intuitive accessibility. There are several drawbacks to this perspective of which the inherent ambiguity is probably the most significant one. Following the typological approach, it is well possible that a completely nonresilient system shows a typical resilient response behavior, while, on the other hand, a truly resilient system may show a degrading performance that has nothing in common with a typical resilience performance curve. The taxonomic (or inductive) approach may overcome some of these problems but is not as intuitively accessible as the typological one. However, in this paper we focus on the taxonomic approach and limit the scope of our work to the definition of resilience in socio-technical systems.

Results: We refer to resilience as a property of systems only to emerge in a state of overload. Overload occurs, as soon as performance requirements (R) exceed the response capabilities (C) of a given. Therefore, overload can be formalized as $C/R< 1$. Furthermore, resilience is defined as the capability of a system to stay productive in an overload state and to overcome the overload state through adaptation. We identified several principles (we call them ”resilience adapters”) that enable the emergence of a resilient reaction, such as fractality, T-shapes or recombinability. Additionally, we found that a resilient reaction can be separated in a degrading phase and an adaptation phase, where each phase utilizes different resilience adapters to generate a resilient reaction. Conclusion: In this paper, we will propose an operational definition of resilience in sociotechnical systems. Some fundamental principles we had found to enable the emergence of resilience will be presented and the pros and cons will be discussed.

Keywords: resilience, definition, framework, adapter, fractal, overload, phases, operational, CD&E, socio, technical, military

EXPERIENCES AND LESSONS FROM DEVELOPING RE METHODOLOGIES

Anthony Smoker[1], Matthieu Branlat, Fredrik London, Lars Danielson, Rogier Woltjer, Billy Josefsson

[1] Lunds Universitet, Division of Risk Management and Societal, Sweden (LTH) – Lund University Box 118 22100 LUND, Sweden

anthony john.smoker@risk.lth.se

A growing critique of the Resilience Engineering (RE) community is that RE is too theoretical for practical use. The SESAR project included two projects developing an RE assessment method. These concluded with it being mandatory in the SESAR safety assessment methodology to assess whether a project will benefit from an R.E. assessment in the design, evaluation and validation process for new ATM system designs.

The first SESAR-RE project established a theoretical position and then developed a method for exploring resilience, validated on a new SESAR ATM concept design. The derived method used workshops, interviews and observations of simulations with operational personnel as the means to explore resilient performance by addressing work-as-done of the current and expected future operation with eight RE principles as a guide.

The second SESAR-RE project applied this method too other SESAR projects– initially Multiple Remote Towers. As a result of this application, the assessment method was determined to require change. The focus in the method changed to operationalising adaptive capacity within the safety assessment.

Candidate methods were identified that were applicable for exploring the sources of resilience, the strategies employed in managing surprises as well as nominal work. A further iteration was undertaken, including the application of an RE method by two Air Traffic Management safety assessors, well versed in the techniques and philosophy of classic safety techniques. Integral in the RE assessment method is a workshop with those actors who are determined to be system actors, thus sources of resilience can be identified and the consequences of drawing upon them derived.

The objective was to integrate an assessment of resilient performance into the safety assessment of the project under study. The two safety assessors were trained in the method and then undertook and facilitated the workshop analysis and results, supported by project team members. The two assessors developed a coding schema that supported the eventual acceptance of hitherto hidden safety implications of the design. In the course of undertaking the research the tension between the approach of research scientists to RE and Safety-II and the safety community immersed in the classic safety background and who are part of the community of intended users of the RE method needed to be navigated.

RE results and narratives therefore need to emphasise the added value that they can bring to not only safety but to effective system performance and within resource constraints. The two practitioners recognised the value that RE can bring to safety assessment, that it may even replace traditional safety approach. These are discussed and the implications for RE practitioners argued. This paper shares the experiences of a project where the objective was to operationalise RE, discusses the issues that arose in terms of RE theory, methodology & politics, proposes the means to navigate these based on the experiences that the RE team had, the principal lessons learned and proposes suggestions for the RE community to embrace in the pursuit of ensuring RE moves from theory to practise.

Keywords: Methodology, Adaptive capacity, Safety Assessment, SESAR, RE

AGENT-BASED MODELLING AND MENTAL SIMULATION FOR RESILIENCE ENGINEERING

Sybert Stroeve[1], Mariken Everdij [1]

[1] Netherlands Aerospace Centre NLR – Netherlands

Agent-based modelling and simulation (ABMS) is an approach for modelling complex systems by describing the behavior and interactions of a collection of autonomous decision-making entities, called agents. The overall system behavior emerges as a result of the individual agent processes and their interactions. ABMS provides a highly modular and transparent way of structuring a model, thus supporting systematic analysis, both conceptually and computationally. An agent-based model of a sociotechnical system describes the performance and interactions of its constituent human operators and technical systems working in an operational context. ABMS offers the possibility to combine a large variety of models for expressing the behavior and performance variability of the interacting agents in a sociotechnical system.

We present ABMS as part of a generic cycle for resilience engineering (RE), including scoping, description of operations, identification of varying conditions, analysis of adaptive capacity, and improvement of resilience [1]. In support of the adaptive capacity analysis, there are two ABMS phases: qualitative ABMS and quantitative ABMS. Qualitative ABMS includes the development of a qualitative agent-based model and it uses this model for reasoning on relations and dynamics of agents' states. The qualitative model development includes the identification of agents and their interactions, and the determination of model constructs as a way to describe the behavior of agents in an operational context. Reasoning on the basis of the qualitative model is called 'mental simulation' and it is used to explicitly identify agents' interactions and to reason about the development of performance variables given particular varying conditions. Quantitative ABMS includes development of a formal model, software implementation and computer simulation.

The approach will be presented in detail for aircraft runway approach operations using conventional systems and an advanced aircraft surveillance application system. We will show by this air transport case that ABMS is a detailed analysis approach for studying resilience of sociotechnical systems that offers a flexible range of model constructs enabling representation of the work-as-done in the system. The agent-based perspective fits well with usual views on elements of a sociotechnical system and it naturally couples states and behavior of the agents.

Preference for an oral presentation

The research on ABMS for RE was published in a journal [2], but is has not yet been presented at a conference. We'd like to discuss this innovative approach with researchers at the REA Symposium.

Acknowledgements

The research reported upon was funded as part of the SESAR Joint Undertaking within P16.06.01b. The views and opinions in this publication are of the authors and are not intended to represent the positions of SESAR JU or its project member organisations.

M.H.C. Everdij, S.H. Stroeve. A practical workshop-based method for resilience engineering. Submitted to 7th REA Symposium, 26-29 June 2017

S.H. Stroeve, M.H.C. Everdij. Agent-based modelling and mental simulation for resilience engineering in air transport. Safety Science 93 (2017) 29-49

Keywords: agent, based modelling and simulation, air transport, infrastructure, safety & resilience

Oral Presentations

Infrastructure, Safety & Resilience

THE EMBRACEMENT OF RISKS. HOW TO MAKE SENSE OF 'RESILIENCE' FOR PUBLIC AND INDUSTRIAL SAFETY?

Juul Gooren [1]

[1] The Hague University of Applied Sciences (HHS) – Johanna Westerdijkplein 75 2521 EN The Hague, The Netherlands, Netherlands

'The capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances' (Zolli & Healy, 2012, p.7) The avoidance of risk to ensure safety and security should not be the primary goal of a community or organisation because that could undermine the primary processes of living in a community or working for an organisation. Safety and security is something that often develops indirectly as a result of involvement. It is under these conditions that a community or organisation will be more resilient. The 'simple, local and diverse' as advocated by Zolli & Healy (2012) resonates as a response to the state-centred view on public safety and the tightly coupled and complex system in industrial safety. In order to be flexible resilience is sceptical of a central and hierarchical organization of safety and security. Furthermore, resilience does not shy away from risk because risks offer all kinds of opportunities and gains. In a similar fashion as cost-benefit analysis resilience understands the management of risks as a trade-off between efficiency vs. fragility and inefficiency vs. robustness (Zolli & Healy, 2012). The logic of resilience has however less to do with predictability as it seems to be a fundamental preparedness no matter what.

Public safety is basically about living together as citizens. Crime and nuisance can be a problem for a community. Industrial safety is basically what organizations have to do in order to make sure that employees return home safely. In every type of organization accidents can happen because of work processes and human error. How to prevent both types of safety and security problems? How about giving people living in a community more responsibility and giving employees working for an organisation more discretionary power? I believe a community police officer and a line manager could learn from one another in how to change human behaviour and create conditions to do so. By focusing on active citizenship in a community and safety culture within an organisation I would like to discover how increasing resilience would work to promote safety and security within both communities and organisations. The purpose of this study is to create an exchange of strategies used in the world of public safety that has been increasingly discussing its concerns in terms of resilience and industrial safety which has been discussing the concept of resilience for many years. I would like to connect recent talk about building resilient communities with the work of resilience engineering. What can both communities and organisations learn from each other in terms of best practices and policy transfers? I think municipalities and corporations can benefit greatly from a cross-fertilization between the domains of public safety and industrial safety. However there are crucial differences between the mentioned social systems making the application of resilience rather problematic. This paper will also emphasis the limits of a catch-all term such as resilience. When does it stop making sense?

Keywords: resilience, risk management, public safety, industrial safety

CREATING FORESIGHT AND RESILIENCE IN EMERGENCY CARE THROUGH REAL-TIME OPERATIONAL 'VITAL SIGNS' AND PREDICTIVE ANALYTICS

Garth Hunte [1]

[1] The University of British Columbia [Vancouver] (UBC) – Canada

Foresight to anticipate and respond flexibly and effectively to changing and unknown conditions is a critical measure of resilience. Forecasting operational demand, with ongoing reassessment and calibration with real-time data, may facilitate foresight in anticipating resource needs to match capability and demand.

The nature of emergency care is to expect the unexpected, and to provide timely response to acute illness or injury. However, the capability to take on new work is limited by crowding and lack of organizational foresight. Mismatch between demand and capacity contributes to prolonged length of stay and adverse patient outcomes, including mortality and hospital admission. This 'falling behind the tempo of operations' - a classic pattern of decompensation in complex systems - is an everyday pattern in an urban ED.

Operational 'vital signs' are real-time metrics that offer an estimate of incoming work, completed work, and work in progress, with the purpose of matching capability/capacity to demand. Key operational metrics that emergency care practitioners use to understand how the department is working are: 1. Total number of patients – metric of crowding; 2. Number of patients in the waiting room – metric of access block; 3. Number of CTAS 2 patients in an unmonitored space – metric of acute resource matching; and 4. Number of patients waiting to be seen – metric of incoming work. Added to this suite of indicators is the evidence based metric of mean ED length of stay – metric of work in progress. These 5 ED 'vital signs' are meaningful real-time operational metrics, but are not easily accessible in one place. We have implemented an hourly electronic printout of these indicators to facilitate proactive system response, including surge response, patient movement, and progress chasing. Further work on electronic data visualization and threshold linked action plans is underway.

Prior efforts to model ED operations have used a variety of mathematical models, but forecast modelling is challenged by the dynamic, state-dependent, and nonlinear nature of inter-actions and interdependencies in the ecology of a complex adaptive system. We are using high dimensional administrative data for all patient visits to six EDs in an urban Canadian health region from April 1, 2014 to March 30, 2016 to build a data-driven predictive model by adapting published methodology. This includes rolling average, LASSO, and K-nearest-neighbor (KNN). By comparing the prediction errors (mean squared error) of those methods, we have found the LASSO predictions to be the most accurate. The average performance of LASSO is comparable to the best prediction error in the literature. We are working on improving the prediction error by exploring other learning-based prediction methods, such as random forest, and nonlinear state-space reconstruction method.

Forecasting operational demand facilitates foresight in anticipating resource needs to match capability and demand. Moreover, it fosters dialogue with stakeholders from community and acute care, and contribute to awareness and anticipatory actions. Data-driven changes are anticipated to lead to improvements in length of stay and patient outcomes.

Keywords: predictive analytics, operational metrics, healthcare, emergency department

FOCUSING ON SUCCESS: A SAFETY-II APPROACH ON OPERATIONAL MANEUVERS IN THE ITAIPU BINACIONAL HYDROPOWER PLANT

Juliano Portela [1], Lia Guimaraes [2]

[1] Itaipu Binacional (Itaipu) – Av Tancredo Neves, 6731 - Foz do Igua¸cu, Parana, Brazil

[2] Universidade Federal do Rio Grande do Sul - UFRGS (BRAZIL) – Brazil

jportela@itaipu.gov.br, liabmg@gmail.com

Serious accidents in organizations with critical infrastructures, such as the Itaipu Binacional Hydroelectric Power Plant, although rare, cause important social and economic impacts in their area of influence. Therefore, they must be avoided even if a ”normal” rate of accidents is expected because of the risk factors and complexity of the operation. This dissertation presents an investigation on the conditions that lead to accidents in the operation of Itaipu Binacional under the proactive approach of Security II management according to Resilience Engineering (RE). It is based on the variability of the normal operation and, therefore, ”in the many things that goes right”, in contrast to the traditional and reactive view of Safety-I, based on the retrospective analysis of accidents and ”the few things that went wrong”. After a review of the literature on the requirements, principles and themes of Security-II, finding inspiration on the FRAM method and on the structured opinions of the operational staff, it was studied the normal operation and variability of four typical operational maneuvers selected by operators within four quadrants of a periodicity-complexity matrix. The results indicated that the same variabilities influence the operational steps, regardless of the complexity or the periodicity of the maneuver. A comparison between the analysis of the variabilities in normal situation and the reports of the four operational failures occurred between 2006 and 2015 indicated that success and failure come from the same source, and that some variabilities such as ”maneuver environment”, ”necessity to confirm the maneuver steps” and ”situations that take the attention of the operator” act decisively in virtually all maneuvers. The results were discussed with the team members who proposed the necessary adaptations to increase the operational safety of normal work from the RE perspective.

Keywords: safety, operational maneuvers, power plant

Oral Presentations

Training Resilience

RECRUITMENT, SELECTION, AND TRAINING OF NEW WORKERS BASED ON RESILIENCE SKILLS: A STUDY WITH GRID ELECTRICIANS

Alexandre Alves [1], Tarcisio Saurin[2], Marcelo Costella[3]

[1] Ftec Faculdades – Brazil

[2] Universidade Federal do Rio Grande do Sul (UFRGS) – Av. Paulo Gama, 110 - Bairro Farroupilha Porto Alegre - Rio Grande do Sul, Brazil

[3] Universidade Comunit´aria da Regiao de Chapeco (UNOCHAPEC´O) – Brazil

saurin@ufrgs.br, costella@unochapeco.edu.br

From the resilience engineering (RE) perspective, the unit of analysis for studying resilience skills (RS) should be the joint cognitive system (JCS) formed by the interactions between the individual professional and their social and material environment. Therefore, data collection for describing RS should account for the context in which they are deployed. The recruitment, selection, and training (RST) of new workers is an important part of this context. In this paper, we discuss the role played by the RST in the use of RS by front-line workers who perform emergency maintenance activities in an electricity distribution company.

The field study involved three main steps: (i) characterization of the requirements posed by the company for recruiting, selecting, and training new workers; (ii) identification of RS demanded by electricians and control room operators; and (iii) crosschecking the data collected in step (i) with the data of step (ii), which allowed evaluating if RS were accounted in the RST of new workers.

Sources of data involved: participant observations; documents that described the RST; twelve interviews through the Critical Decision Method; data regarding the performance of workers who participated in the RST, including 450 applicants for the electrician job and 80 for the position of control room operator. Interviews and notes from observation diaries were subjected to a content analysis, in which RSs and the work constraints which triggered their use were identified.

With respect to results of step (i), the company demanded a number of technical and educational background requirements, psychological tests, medical examinations and physical tests. For the electrician job, applicants who had been approved in the initial psychological and medical tests (i.e. 215 out of the initial 450 applicants) attended a 360 hour training course, at the end of which they could be eventually hired or not.

As to findings related to step (ii), 11 categories of RS and 10 categories of work constrains were identified. These RS were checked against the requirements of the psychological tests used by the company over the RST process, both for the electricians and for the control room operators (step iii). This comparison indicated that all of the 11 RS were at least partially covered by the psychological tests, even though these had greater emphasis on personality traits, reasoning and memory. Also, results indicated that, provided some RS had not been considered over the RST process, this would imply the creation of some of the identified work constraints in the future.

In fact, the company's training coordinator acted so as the RS and work constraints identified in this study were accounted by instructors during the electrician's training course. This made the practical training sessions more likely to demand the use of RS. As a result of these changes, 10% of the 215 applicants were considered as inapt during this late stage of the RST process. This is contrast with the 1% failure rate that was previously common in the company.

Keywords: Resilience skills, training, electricians, recruitment and selection

SERIOUS GAMES: AN EfficIENT TOOL FOR THE LEARNING ABOUT CITY RESILIENCE

Marta Iturriza [1], Leire Labaka, Jose Mari Sarriegi

[1] University of Navarre (University of Navarre) – Tecnun, Paseo Manuel Lardizabal 13, 20018, Donostia, Spain

The relevance of resilience has increased significantly over the last years as both natural and man-made disasters have augmented. Moreover, as cities continue to grow, there is a need of building cities resilience, not only in a theoretical but also in a more practical way. There are several studies that define resilience policies and actions in order to achieve higher resilience levels1. However, none of these studies explain the inter-relations existing between the policies and the way they must be implemented. In parallel, the use of serious games (SG) for didactical objectives has also been a significant topic lately. Due to the appearance of new technology, the way humans communicate, learn and teach have changed. Moreover, by having new technological tools, learner's profile changes and demands a more interactive way of learning 2. In light of this situation, tools such as SG are commonly used. While some experts define SG as a non-usable and ineffective tool, others claim SG environment can promote learning and motivation, providing features that prompt learners actively process the learning content3.

Taking both realities into account, the aim of this research is to develop a successful serious game with the objective of training cities to be more resilient. Through the SG decision makers and crisis managers will be taught which way is the most effective to achieve resilience and will understand the inter-relationships existing among the policies.

The serious game is based on a maturity model that defines the path cities need to follow in order to improve their resilience level. The maturity model is structured in five maturity stages achieved by cities in a systematic and incremental way through the stakeholders' involvement. Each maturity stage is defined by different policies stakeholders need to implement to progress. Furthermore, all the presented policies are inter-related and therefore, depending on the order in which policies are applied, the efficiency of the implemented policies will vary and thus, different results will be achieved.

Furthermore, the structure of the game is divided in two main parts; a system dynamic (SD) model and the interface. On the one hand, an user friendly interface is created as an intermediary between the user and the SD model. The input data will be introduced through the user interface and the results of the simulation will be represented in a more visual and understandable way. On the other hand, a system dynamic model is developed where the simulation is carried out based on the input introduced by the users. The SD model contains the structure of the model taking into account all the inter-relations and the temporal order of the policies and it simulates the evolution of the resilience level over time.

Developing successful serious games to train pedagogically cities being more resilient is of utmost importance and incipient in the field of crisis management. This research goes a step further developing tools that will support the learning of the cities in the resilience building process.

Keywords: Critical infrastructures, inter, dependencies, system dynamic, simulation

SIMULATION GAMES FOR DEVELOPING COMPLEX SYSTEMS THINKING SKILLS AND STRENGTHENING ADAPTIVE CAPACITY

Lauren Mcburnett [1], Margaret Hinrichs [1], Susan Spierre Clark [1], Thomas Seager [1]

[1] Arizona State University, Tempe, AZ, USA – United States

lauren.McBurnett@asu.edu

Resilient infrastructure requires people that are capable of thinking in complex systems ways. Since actionable resilience depends upon the processes of sensing, anticipating, adapting, and continuous learning, the adaptive capacity of individual decision makers relies upon their understanding of the complexity. Existing academic and training programs provide inadequate focus on developing the complex systems thinking skill which are necessary for infrastructure managers to address the US infrastructure crisis. We learned from the Kolb Learning Cycle that there are four stages required for transformative learning: abstraction, experimentation, experience, and reflection. Experiential learning, which requires real-world context, is lacking in current educational platforms because it would be impractical or impossible to stage infrastructure crisis conditions. We cannot stage a week-long power-outage to provide training opportunities to engineers and infrastructure managers. Even within the real-world systems, some infrastructure failures occur over hundred year periods. This means that multiple generations of decision makers never experience the task of managing the infrastructure system during the failure conditions. We propose the use of simulation games for teaching complex systems thinking skills. Because simulation games can imitate the conditions of short and long-term infrastructure failures, decision makers can experience the complete lifecycle of infrastructure management.

We developed a series of infrastructure simulation games which teach four components of complex systems thinking skills: (i) interdependencies, (ii) feedback loops, (iii) nonlinearity, and (iv) stochasticity. The first game is The LA Water Game, which teaches the feedback loop between the LA water distribution system quality, public opinions, and funding. Students play the generational role of the LA Water Manager and are tasked with managing the LA water distribution system without being fired. This task is difficult because the complex system behaves in nonlinear ways and players' decision fall subject to stochastic pipe break events. Power-Water Game, teaches interdependencies between the power and water systems by illustrating how the power and water systems are effected by climate changes. The third game is the Water Sustainability Climate Game, which teaches how vulnerabilities in the power and water systems are interdependent and demonstrates how strategic investments can be made to mitigate the consequences of climate driven vulnerabilities. To establish the validity of the simulation game method for teaching complex systems thinking skills, it is import to assess and substantiate what students learn during the games. We propose a concept mapping activity to assess students' understanding of complex systems pre and post game play. Students interviewed will be conducted to complement the concept mapping assessment. The LA Water Game has been piloted in ten group work-shops with more than 100 individuals. First, we observed that students' prior experiences and disciplinary training impacted the students' performance. Second, The LA Water Game revealed to students the generational inheritance of infrastructure problems. Lastly, after playing The LA Water Game participants demonstrated new understanding of infrastructure systems and acquired appreciation for complex systems thinking skills. The simulation game provides a context rich with potential for complex systems thinking skill development, as well as engaged learning through all four stages of the Kolb Learning Cycle.

USING SIMULATION GAMES TO ASSESS THE RESILIENCE OF CRITICAL INFRASTRUCTURES IN THE PAYMENT SYSTEM

Joeri Van Laere[1], Björn Johansson[2], Peter Berggren[2]

[1] University of Sk¨ovde – Sweden 2 Link¨oping University – Sweden

joeri.van.laere@his.se, bjorn.j.johansson@liu.se, peter.berggren@liu.se

Infrastructures for fuel, food and payment systems become increasingly entangled [1] in dependencies on each other and a large variety of support systems as well as other systems that provide services crucial for the function of the overall system. When a disturbance occurs, the resilience of these infrastructures depends more and more on the ability to produce collaborative responses from individuals with diverse backgrounds that may not be familiar with side impacts in totally different areas. Resilient behavior through collective action patterns of involved stakeholders allows for dealing successfully with disruptions in these critical infrastructures. Given the variety of interpretations of resilience [2], resilience is hard to operationalize into measurable indicators [3]. Lundberg and Johansson3 have therefore proposed the Systemic Resilience (SyRes) model as a way to describe process, functions and strategies on a conceptual level in an effort to synthesize different perspectives in the field of resilience research. Weick and Sutcliffe [4] describe resilient behavior as anticipation through ”reluctance to simplify” and ”action in order to think more clearly”. It may seem contradictory that Weick and Sutcliffe argue for sensitivity to operations and reluctance to simplify (i.e. an interest in details and scrutinize the situation at hand) while encouraging simultaneous blunt and immediate action without thorough analysis. The way out is that the deep knowledge about the system should have been acquired earlier (long before the disruption) so that in case of disruptions quick and blunt action is possible based on deep understanding of the system's dynamics.

This paper presents initial findings from a project aiming to develop a gaming simulation (a combination of role playing games and computer simulation) that can be used to better understand the complex dynamics in the payment, food, fuel and finance system. The purpose of developing the gaming environment is to train decision-makers in handling crisis situations in a multi-organisational context. Gaming simulation [5] aims at representing reality and enabling an individual actor or a group of actors to experience the dynamics of the simulated system. The SyRes model will be used to guide the simulation approach so that all core functions of a resilient system, as well as coping strategies, will be addressed in the gaming sessions.

Ansell, C., Boin, A. and Keller, A. (2010). Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System. Journal of Contingencies and Crisis Management, 18: 195–207.

Bergstrom, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. Reliability Engineering & System Safety. 141: 131-141.

Lundberg, J., & Johansson, B.J.E. (2015) Systemic Resilience Model. Reliability Engineering and Safety Science. 141, 22-32.

Weick, K.E. and Sutcliffe, K.M. (2007). Managing the unexpected. Resilient performance in and age of uncertainty. Jossey Bass, San Francisco, 2nd edition.

Laere, J. van, Vreede, G.J. de, and Sol, H.G. (2006). A social simulation game to explore future coordination in knowledge networks at the Amsterdam Police Force, Journal of Production Planning and Control, 17(6) 558-568

Oral Presentions

Resilience in Aeronautics and Space Systems

ABNORMAL AND EMERGENCY SITUATIONS IN AVIATION: IMPROVING THE QRH TO SUPPORT RESILIENCE

Guido Cesar Carim Junior [1,2], Tarcisio Saurin [3], Eder Henriqson [1]

[1] Pontif´ıcia Universidade Cat´olica do Rio Grande do Sul (PUCRS) – Av. Ipiranga 6681 - Porto Alegre, Brazil

[2] Azul Airlines (Azul) – 939 Marcos P.U. Rodrigues Avenue, Barueri-SP, Brazil, Brazil

[3] Universidade Federal do Rio Grande do Sul (UFRGS) – Av. Paulo Gama, 110 - Bairro Farroupilha Porto Alegre - Rio Grande do Sul, Brazil

jrguido@gmail.com, saurin@ufrgs.br , ehenriqson@pucrs.br

Commercial airlines are known for using highly reliable technology and highly-standardized operations which reduce uncertainty, variability and risks. The systems resulted from these approaches are effective to handle well-defined problems[1] for both normal and abnormal operations. For the latter is expected that: pilots identify the problem; choose, read and understand the contents of the Quick Reference Handbooks (QRH) checklist , execute the steps; and evaluate the results[2]. The rationale behind traditional QRH is that anomalies and emergencies can be addressed by using one checklist for each situation[3]. However, what if pilots face situations that cannot be solved following the prescribed sequence or not covered by the selected checklist in the QRH? Our previous study[4] with pilots from a major commercial airline has shown that the successful management of ill-defined emergencies and anomalies lies on the strategies deployed by the cockpit based on the interactions between a range of ”resources for activity (RfA)”, which include but are not limited to the QRH. Since not all circumstances are covered by the QRH, the cockpit interweaves strategies supported by fragments from different RfA in order to deal with the problem while trying to concurrently manage the flight.

Hence, this study suggests improvements in the QRH design, so as it can interact more effectively with other RfA, and thus support the cockpit to manage both well and ill-defined anomalies. In particular, we propose to transform the paper-based QRH in an electronic tablet-based information system (which allows for dynamic properties) with the following functionalities:

• The system must be ready to be used when needed and it must include feedforward mechanisms (e.g. predicting what might go wrong based on past maintenance reports).

• The QRH should concurrently aid the cockpit to make sense of the nature of the failure, to diagnose the probable cause(s) of disturbances and to act therapeutically or diagnostically. • For time critical emergencies, the QRH should provide ready-to be-used checklists and elect, suggest and provide guidance for the nearest suitable airport(s). • Whenever the failure compromises the aircraft performance, the QRH should display landing performance calculator. • It should be possible to remotely modify and manage the QRH, thus reducing the time required to update. • Passive and active feedback from users and recent events should allow continuous improvement of the QRH. In this case, ”machine-learning technologies” should be considered.

Woods, D.D., 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering and System Safety, 141, pp.5–9.

Civil Aviation Authority (CAA), 2006. CAP 676: Guidance on the Design, Presentation and Use of Emergency and Abnormal Checklists, London, England: CAA.

Burian, B.K., 2006. Design Guidance for Emergency and Abnormal Checklists in Aviation. In Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting. San Francisco, CA, USA: Human Factors and Ergonomics Society, pp. 1–6.

Carim Jr., G.C. et al., 2016. Using a procedure doesn’t mean following it: A cognitive systems approach to how a cockpit manages emergencies. Safety Science, 89, pp.147–157.

Keywords: procedures. anomaly management, abnormal, emergency, quick reference handbook, QRH, aviation

FLEXIBLE PROCEDURES TO DEAL WITH COMPLEX UNEXPECTED EVENTS IN THE COKPIT

Joris Field, Amy Rankin [1], Rogier Woltjer [2], Frederik Mohrmann, Edzard Boland, Jeroen Van Rooij

[1] Department of Computer and Information Science - Linkoping University – SE-581 83 LINKOPING SWEDEN, Sweden

[2] Swedish Defence Research Agency (FOI) – Sweden

joris.field@nlr.nl

Modern flight crew operate in an environment with multiple detailed procedures to cover critical abnormal events, and with systems that are automated and highly reliable. Complex and unexpected events without a clear procedure or systems solution are rare, and may thus present a challenge to the crew in knowing how to assess the situation and decide on a course of action. However, unexpected events still occur, and can in some cases be complex, which may adversely affect the crew's ability to react and deal with the event. An example of this is the engine explosion that occurred on Qantas Flight 32 leading to a multiple systems failure. The accident exemplifies how an experienced flight crew initially try to apply procedures as required, but eventually needed to adapt their response to the situation that they faced and be flexible in the application of the procedures. In the recently completed "Man4Gen" EU project the flight crew's ability to respond to unexpected events was investigated in a series of simulation experiments, with an aim to identify strategies to assist the crew in dealing with complex situations with multiple system failures. Initial experiments with 20 crews were used to identify strategies applied by different crew in dealing with situations were no single procedure was applicable and thus required a certain amount of problem solving and decision making. The experiment scenarios included complex unexpected events, such as a bird strike that caused problems on multiple engines. The aim of these scenarios was to create a situation with multiple conceivable options for strategies of how to cope with a problem, where there was no single correct strategy based on normal operating procedures. The findings were then used to develop a guide in the form of a flexible procedure that would assist crews in responding to events for which there was no single, clear, procedure. This flexible procedure was evaluated in a second set of experiments in a simulated operational environment with 18 crews from several international airlines. This paper describes the development and evaluation of the flexible procedure based on the strategies that were applied by operational flight crew responding to unexpected and complex events in flight scenarios. The outcome of the initial experiments identified the strategies and competencies that were most beneficial to the resilience of the crew in the experiment scenarios. It is these strategies – problem solving, decision making, leadership, communication – that formed the basis of the separate steps in the flexible procedure. The result focuses on three phases to manage time criticality, manage (un)certainty, and finally to plan for contingencies and changes. These phases were translated into steps in a procedure that can be used by flight crew to assist them in responding flexibly and therefore to a variety of events. This forms the basis of the discussion of how training procedures can be used to assist resilience in the cockpit, rather than forming a barrier to it.

Keywords: Aviation, Flight Crew, Flexible Procedure, Unexpected, Training

CONCEPTUAL AND COMPUTATIONAL MODELLING OF COORDINATION MECHANISMS IN AIR TRAffiC MANAGEMENT

Mannat Kaur [1], Alexei Sharpanskykh [1]

[1] Aerospace Engineering - Delft University of Technology – Netherlands

The commercial air transportation system comprises many different interacting with each other human actors, such as pilots, actors in Air Traffic Control (ATC) centers, at airlines and at airports. The effectiveness and efficiency of coordination and communication between these actors is essential for achievement of the very high safety records of modern commercial air transportation. Commercial air transportation is a highly regulated system where the coordination procedures for human actors are well defined up to a certain procedural level. However, in practice nonnominal situations occur for which the set of existing procedures fall short, as a result of which human actors coordinate informally in a partially improvised way. Evidences exist that such an improvised coordination is often successful in practice.

Understanding of generic coordination mechanisms and their breakdowns in sociotechnical teams has been a long-standing challenge, in particular in the areas of human factors and social sciences. A few theories and conceptual frameworks were proposed to describe and explain coordination in teams. However, formal, systematic modelling of coordination in sociotechnical teams is still very limited; strengths and weaknesses of such approaches are not well explored.

In this paper we elaborate coordination processes in ATM using three existing modelling tools: a conceptual model of joint activity (Klein et al., 2004), a conceptual co-ladder model of coordination (Chou et al., 2000), and a formal framework for multiagent situation awareness relations (Blom and Sharpanskykh, 2015). These modelling tools address coordination at different levels of abstraction ranging from abstract conceptual to detailed formal. In the paper we demonstrate how these modelling tools can complement each other, and how by integrating them in a unifying framework a more profound understanding of coordination mechanisms can be achieved. We illustrate this framework by elaborating an ATM scenario, in which multiple non-nominal hazardous situations occurred, and the actors needed to coordinate with each other to handle these situations. A special focus of this study has been on coordination mechanisms related to maintaining common ground, identification of loss of common ground and its repair. Common ground refers to pertinent knowledge, beliefs and assumptions that are shared among the ATM actors.

Based on the elaborated coordination model we developed an agent-based simulation model, which was used to study the dynamics of coordination mechanisms in different variants of the ATM scenario using 'what if' simulation.

Among the identified mechanisms that help maintaining common ground among actors in ATM are: acknowledgement/readback of a plan or activity, comparison of expected states attributed to other agents with the observed behaviour of these agents, requesting/providing information when state certainty is low or outdated, reasoning based on communication among other agents involved in the joint activity, group discussion and exchange of stances of agents about disputable issues. The proposed approach and the identified coordination mechanisms related to common ground could be used to improve training of actors in ATM. Another possible application is in automated support facilitating coordination in ATM. Such automated systems could alert actors when a possible loss of common ground is detected.

Keywords: coordination, air traffic management, agent based modelling and simulation

RESILIENT DECISION MAKING IN THE COCKPIT: DOES IT WORK?

Frederik Mohrmann[1], Joris Field [1], John Stoop [2]

[1] Netherlands Aerospace Centre (NLR), Amsterdam, the Netherlands – Netherlands

[2] Kindunos Safety Consultancy, Gorinchem, the Netherlands – Netherlands

frederik.mohrmann@nlr.nl

This paper evaluates a novel complex situation management strategy for flight crews in civil aviation. This strategy has been developed and evaluated in the EU-funded research project Manual Operations of Fourth Generation Airliners (Man4Gen), which investigates crew recovery capabilities in modern airliners. Based on exploratory simulations earlier in the Man4Gen project, the strategy attempts to provide crews a method to assert themselves effectively in complex, unexpected and ambiguous situations. Nestled within the philosophy of resilient operations in an increasingly complex operational context, the strategy will guide crews where conventional procedural resolutions and brittle and fall short. The design process of this strategy is detailed in a related paper by Field, Mohrmann and others, also submitted to the REA. The Man4Gen project investigated whether introducing this new strategy would in fact result in increased performance. This experiment enlisted 17 Airbus A330 & A320 type-rated crews from various airlines and challenged them in a carefully refined scenario providing a complex energy management issue and an emergency diversion in bad weather. An important scenario element was the perceived (but not actual) time pressure. Crews were evaluated on 30 distinct challenges and risks to be managed throughout the scenario involving both engine management and navigation. These performance metrics would then be compared to a behavioural analysis which observes whether crews performed the strategy's steps, and in which order. This comparison would be able to conclude whether applying the strategy as design actually leads to an increase in situation management performance.

Performance analyses (ANOVA, 0.05 level) revealed that the original test groups (trained vs not trained) did not exhibit strong group distinction in performance, but rather featured an overlapping spectrum of performance. As the strategy only served as an intervention to introduce higher performance, the crews were regrouped into high and low performing crews. The new groups featured low within group variance, and high between group variance. The subsequent temporal behavioural analysis observed the actual detailed steps of the strategy, as well as the abstract level of strategy's philosophy. Analysing their behavioural trends revealed that there were distinct differences in the behavioural patterns of high and low performing crews. Performance increase correlated with stricter task sequencing along the strategy, not skipping steps or revisiting past steps, as well as increased use of the latter half of the strategy (managing uncertainties and contingency planning). At an aggregate philosophy level, the analysis reinforced the effect of strict sequence, expediting time management and taking time for contingency management. This study concludes that the Man4Gen situation management strategy does indeed provide crews with effective guidance when addressing complex and ambiguous scenarios. In this way, this strategy is a concrete attempt to operationalize resilience theory in an industry which is becoming increasingly challenged by complexity which often trumps brittle Taylorist approaches to threat and error management. By engaging the human ability to learn, understand and anticipate, this strategy leverages the human asset in the cockpit, and sets an example for further operationalization of resilience theory.

USING THE RAG TO ASSESS INTERNATIONAL SPACE STATION ORGANIZATIONAL RESILIENCE

Christopher Nemeth [1], Beth Lay

[1] Applied Research Associates, Inc., VA, USA – United States

Elizabeth.A.Lay@hotmail.com

Understanding high risk work settings from the viewpoint of resilience engineering (RE) requires methods that enable the researcher to successfully collect and analyze data, then provide well-founded findings and recommendations. We report on our experience using one RE method, the Resilience Analysis Grid (RAG) (Hollnagel, 2011), as part of an assessment of the organizational resilience of the role the U.S. National Aeronautics and Space Administration (NASA) plays as a partner in the International Space Station (ISS) Program. Two events led to the study. Each occurred during the performance of an extra vehicular activity (EVA), or spacewalk, outside of the ISS. In both cases, water was observed to accumulate in an astronaut's helmet. In the second instance, EVA 23, it became evident that the accumulation of water in the space suit's closed system could become life-threatening and the spacewalk was terminated. In response to recommendations from a mishap investigation board (MIB, 2013) report of the EVA 23 incident, the ISS Program Office invited the NASA Engineering and Safety Center (NESC) to assess how the agency handled this and similar situations, in order to improve its work processes. The NESC organized a team comprising five human factors specialists, working within NASA as civil servants or contractors, and two RE specialists from outside NASA. The team leader selected the RAG as the tool to analyze NASA system performance using EVA 23 as a case study. The team used the four RAG cornerstones (anticipate, monitor, respond, learn) to structure data collection, analyses, and findings.

The team: • Reviewed artifacts to learn actions that have and are being taken in response to recommendations from past mishap investigations and incident reports, • Conducted a series of interviews with crew members and mission control center operational and engineering staff members • Observed several groups at Johnson Space Center during 3 spacewalks. • Performed a thematic analysis of interview and artifact data • Provided recommendations for the ISS program regarding its resilience traits, based on our assessment of current practices, including recommendation to improve work processes.

Our presentation will reflect on the application of the RAG to study a complex, high risk work setting. We will also share our experience with introducing team members to RE in general, as well as RAG in particular. For example, more than once we heard the question ”Are these the ”official” or sanctioned principles of RE?” This begs the question of how novice practitioners can be introduced to and undertake RE study without a background in the RE literature. We will conclude with a review of how well RAG served the team, what the team needed to use it well, and provide observations on the evolution of RE field study based on our experience.

PREVALENCE OF RESILIENT SKILLS IN GENERAL AVIATION CREWS

Arjun Rao[1], Shawn Pruchnicki [2,3], Seth Young [1]

[1] The Ohio State University, Center for Aviation Studies – United States

[2] The Ohio State University, Center for Aviation Studies – United States

[3] The Ohio State University, Department of Integrated Systems Engineering – United States

rao.119@osu.edu

General Aviation (GA) is a catchall term for all aircraft operations in the United States (U.S.) that are not categorized as commercial operations or military flight. The International Civil Aviation Organization (ICAO) defines GA operations as "as all civil aviation operations other than scheduled air services and non-scheduled air transport operations for remuneration or hire"[1]. In the U.S. in 2014, GA aircraft comprised approximately 97% of the aviation fleet. Recent estimates by the Federal Aviation Administration (FAA) showed that the GA fatal accident rate has remained relatively unchanged between 2010 and 2015, with 1566 fatal accidents accounting for 2650 fatalities during this time[2]. Traditionally, the literature base for this domain has focussed on identifying resilient skills and strategies employed by crews in commercial aviation operations. However, in this paper, we seek to supplement several research efforts that have been directed towards better understanding of the causes of GA accidents. Understanding the behaviour of pilots/crew plays a critical role in potentially better understanding of the causes for both fatal and non-fatal GA accidents. Specifically, in this paper we seek two answers to the following questions: (1) How many fixedwing GA accidents involved "surprise" or "unexpected events"?; (2) Did the pilots/crew in these accidents demonstrate resilient skills?

To answer the first question, we analyze historical accident data from the National Transportation Safety Board (NTSB) database. We analyze fixed-wing GA accidents that occurred in the US between 1982 and 2016. We identify accident reports that suggest that pilots encountered surprise/unexpected events during aircraft operation. We argue that analyzing non-fatal GA accidents (approximately 86% of GA accidents in the U.S.) could provide additional insight into the skills demonstrated by pilots. For the second question, we carry out an in-depth analysis of factual accident reports using the resilience indicators presented by Wachs et al.[3], Dekker and Lundstrom[4], and Grøtan et al.[5], to determine if pilots demonstrated sign of resilient behaviour.

We propose that eventually the value of this research will be evidence that certain resilient skills are in fact helpful in potentially mitigating undesirable outcomes. Especially for those events that could be labelled as unexpected. Thus, once this is understood with supporting evidence, training organizations will finally have empirical support and thus a better grasp on skills that could be taught during all levels of airman certification. The focus of this effort will be that if more pilots possess these skills once trained, then these abilities acquired by all airmen may help to finally decrease the stagnant GA accident rate in the U.S.

International Civil Aviation Organization (2009). Review of the classifications definitions used for civil aviation activities. Tenth Session of the Statistics Division, STA/10-WP/7, Montreal, Canada, November 2009.

Rao, A. H. (2016). A New Approach to Modeling Aviation Accidents. Ph.D. Dissertation, Purdue University, West Lafayette, IN.

Wachs, P., Saurin, T. A., Righi, A. W., & Wears, R. L. (2016). Resilience skills as emergent phenomena: A study of emergency departments in Brazil and the United States. Applied ergonomics, 56, 227-237.

Dekker, S. W., & Lundstrom, J. (2006). From threat and error management (TEM) to resilience. Human Factors and Aerospace Safety, 6(3), 261.

Grøtan, T. O., van der Vorm, J., & Macchi, L. (2015). Training for Operational Resilience Capabilities (TORC): 1st Concept Elaboration. SINTEF Technology and Society, Trondheim.

Posters' Abstracts

BOXING AND DANCING - THE CHALLENGES OF ENFORCEMENT IN GLOBAL SHIPPING

Nippin Anand [1]

[1] Safety Management System, DNV GL - Maritime – Netherlands

Nippin.Anand@dnvgl.com

The author propose to present his paper entitled "Boxing and dancing - The challenges of enforcement in global shipping". Read the paper to have a precise idea of the thematic broached.

SIMULATED EXERCISES IN EMERGENCY RESPONSE A RESSOURCE TO RECONCILE WAI AND WAD

Paulo Carvalho [1], Jose Orlando Gomes [2], Angela Righi [2], Gilbert Huber [2], Caio Lemos [2]

[1] Instituto de Engenharia Nuclear (IEN) – Brazil

[2] Universidade Federal do Rio de Janeiro (UFRJ) – Brazil

In this work we analyze two simulation exercises in emergency response performed as part of a training program for officers of the Fire Department of the State of Rio de Janeiro. The simulations had different formats1: tabletop type (June 2015 with 35 officers) and functional exercises (November 2015 with 40 officers). Both have the same script and purpose – verify the management of an operational event (emergency response) by Firefighters officers, while using the Standard Operating Procedures (SOPs) developed by the corporation – but with different features due to their format. The exercises were running from an initial scenario, and new information was inserted to trigger officers' actions to deal with unfolded escalating situations. Data collection and analysis followed the methodology of cognitive task analysis2 including direct and non-participative observation, and audio and video recording of the simulation. The material was analyzed by the research team, which sought to understand work as imagined (WAI) and work as done (WAD) during the exercise, as well as aspects of resilience in that context. Validations of the results were performed by Firefighters experts.

Both exercises presented common insights, even with their different simulation format. This fact indicates that the observations of simulations exercises allowed to partially understanding the WAD, contributing to rethink on the WAI and the SOPs design. Our main findings were the dependence of the context for the decision making and the acknowledgment of the insufficiency of the SOPs through these different contexts.

In the first simulation, two moments exemplify this finding: at the beginning of the simulation, a request for police support was made before arrival at the emergency site, and later, the absence of a new request was verified, although it was justified. The first request was made by an officer with knowledge of the region to which they were addressed and who knew from experience that it would be necessary. In the second case, involving an officer that works in a rural area, showed the difference between operating inland, where additional support may take up to two hours to reach, from the ones that operate in urban areas, where the police support can be in place in a relatively short time. These are examples of resilient actions related to the knowledge of each officer that extrapolates the instructions. In the second exercise we found the difficulty of SOPs in guiding those responsible for actions in a clear way in each scale of an escalating event. This appear when officers fail to realize the situation was escalating to higher level, and thus identify to whom report. Another example concerns the difficulty of following the guidelines of the SOP when the actual situation does not have adequate information and/or means to do so. Sometimes the officer in command did not have knowledge on the resources available at the site, hindering the situational awareness of all, mainly due to the lack of registration of the previous actions taken and the lack of communication support to aid in the sharing of information.

Keywords: emergency response, simulations exercises, wai and wad, firefighters

REDEfiNING AND MEASURING RESILIENCE IN EMERGENCY MANAGEMENT SYSTEMS

Son Changwon [1]

[1] The Department of Industrial and Systems Engineering, Texas AM University – United States

Emergency management system (EMS) provides a crucial barrier for the protection of socioecological infrastructure from man-made disasters and natural threats. To meet diverse demands from hazardous events, resilience engineering is considered as an effective approach to enhance the performance of EMS. While conceptual and qualitative descriptions of resilience are abundant, ideas of operationalizing resilience are scarce. In this regard, this poster presents an attempt to redefine resilience in the EMS and propose a framework of measuring resilience by abstracting the EMS as a joint cognitive system.

SOME IMPLICATIONS OF BONE'S BIOLOGICAL FEATURES FOR SYSTEMIC RESILIENCE

Richard Cook [1]

[1] Ohio State University (OSU) – Ohio State University Enarson Hall 154 W 12th Avenue Columbus, Ohio 43210, United States

To understand resilience in large, deliberately constructed systems it may be useful to examine it in smaller, naturally occurring ones. The development, maintenance, and repair of bone is one such system. At both the micro- and macro-scales, bone dynamics demonstrate the functions, costs, and limits of resilience. Development of the skeleton is carefully orchestrated and maintenance and repair continue throughout life. Bone is a storehouse of the organism's calcium - the most important inorganic elements. The turnover of bone is tied to calcium homeostasis. Far from being a static, inanimate, mechanical frame, bone is a richly innervated, highly perfused, and has a subtly complicated structure.

The organism is constantly resorbing and replacing bone along lines of stress. This optimizes the mechanical strength while limiting weight and preserving scarce minerals elements. In combination with the body plan this results in regular skeletal features including emergent architecture for specific bones. Overt damage (e.g fracture) produces cascading repair mechanisms that involve several different pathways that can take years to resolve. Influences on bone resorption and creation are integrated locally and globally.

Bone system resilience is both limited and susceptible to failure. Bone disorders arising from molecular defects, various cancers, and faults in signaling associated with abnormal organ function can lead to disorganization, disruption, or depletion of bone. Studying the array of disorders provides insight into the mechanisms of resilience and the patterns may suggest general properties of resilience.

Some features related to resilience include:

The presence of both programmed and emergent features Having continuous, directed replenishment rather than periodic or episodic renovation Localized signaling that can garner and make use of resources for damage control. The ability to sacrifice lower level goals (e.g. mechanical strength) for higher level ones (e.g. maintenance of serum calcium levels) Susceptibility to disruption by loss of internal regulation (e.g. the effects of parathyroid adenoma)

The existence of a naturally occurring resilient system and the detailed physiological, and now, molecular biological models of that system provides avenues for more general study of resilience. The poster and proceedings paper will sketch the nature of bone resilience and suggest connections to resilience engineering work at other scales.

Keywords: systems biology, bone, calcium homeostasis, remodeling, goal hierarchy

PROJECT RESOLUTE - ENHANCING RESILIENCE IN URBAN TRANSPORT SYSTEMS

Pedro Ferreira [1]

[1] CENTEC – IST, University of Lisbon – Portugal

ferreira.pnp@gmail.com

Increasing Europe's resilience to crises and disasters is a topic of highest political concern in the EU and its Member States and Associated Countries. Regarding the specific case of transport systems, it can be said that those have developed a prominent safety and business critical nature, in view of which current management practices have shown evidence of important limitations in terms of resilience management. Furthermore, enhancing resilience in transport systems is considered imperative for two main reasons: such systems provide critical support to every socio-economic activity and are currently themselves one of the most important economic sectors and secondly, the paths that convey people, goods and information, are the same through which risks are propagated.

RESOLUTE is based on the vision of achieving higher sustainability of operations in European UTS. The project recognises foremost the ongoing profound transformation of urban environments in view of ecological, human and overall safety and security needs, as well as the growing importance of mobility within every human activity. Sustainability is rapidly becoming an imperative need across all economic and social domains. Among many things, this requires overall heightened operational efficiency, mainly by optimising the allocation and utilisation of available resources (organisational technical and human), whilst striving to continuously minimise any source of waste, namely incidents, accidents and other operational failures.

Within this context, RESOLUTE considers resilience as a useful management paradigm, within which adaptability capacities are considered paramount. Rather than targeting continuous economic and financial growth of businesses and market shares, organisations must generate the ability to continuously adjust to ever-changing operational environments.

RESOLUTE is answering those needs, by proposing to conduct a systematic review and assessment of the state of the art of the resilience assessment and management concepts, as a basis for the deployment of an European Resilience Management Guide (ERMG), taking into account that resilience is not about the performance of individual system elements but rather the emerging behaviour associated to intra and inter system interactions. The final goal of RESOLUTE is to adapt and adopt the identified concepts and methods from the defined guidelines for their operationalization and evaluation when addressing Critical Infrastructure (CI) of the Urban Transport System (UTS), through the implementation of the RESOLUTE Collaborative Resilience Assessment and Management Support System (CRAMSS), that adopts a highly synergic approach towards the definition of a resilience model for the next-generation of collaborative emergency services and decision making process.

BENEFICIAL INTERRUPTIONS IN THE EMERGENCY DEPARTMENT

Katherine Forsyth [1], Rachelen Varghese [2], Nibras El-Sherif [1], Hunter Hawthorne [1], Renaldo Blocker[1]

[1] Department of Health Sciences Research [Mayo Clinic] (HSR) – Mayo Clinic 200 First Street SW Rochester, MN 55905 USA, United States

[2] Department of Emergency Medicine [Mayo Clinic] (EM) – Mayo Clinic 200 First Street SW Rochester, MN 55905 USA, United States

forsyth.katherine@mayo.edu

Introduction: Work system interruptions in the emergency department (ED) threaten patient safety, since interruptions disrupt clinicians' cognitive processes and increase their cognitive demands, thus increasing the risk for committing errors. Identifying the positive uses of interruptions in the ED though demonstrates the the system's ability to succeed under both expected and unexpected conditions. Therefore, the present study prospectively examined the characteristics of interruptions in the ED with respect to current protocols and whether the interruption was considered appropriate. Method: Interruptions of attending physicians were prospectively collected in the ED at one academic institution. Convenience sampling was used to select the location (i.e. wing) in the ED observed. Data included the description of the interruptions, the clinicial role of the interrupter, and location of the interruption. Following the data collection, the interruptions were categorized thematically. Insitutional procedures were also reviewed to determine whether or not relevant protocol existed and whether the interruption was appropriate. Interruptions were considered appropriate when its purpose was pertinent to the patient's continuing care and necessary for the physician to be updated.

Results: Across 16 hours of observation, 22 interruptions of the attending physician occurred. Six interruptions occurred in the pediatric wing and the remaining interruptions occurred in the main adult wing. Eight of the identified interruptions (8/22, 36.4%) were considered appropriate. Nurses and residents interrupted ED physicians regarding patient updates (3/8, 37.5%), ordering patient tests (2/8, 25%) the lack of beds for admitting (3/8, 37.5%). Only three of the interruptions had a relevant protocol that was followed (ordering patient tests and one patient status update). Discussion: Interruptions can have both positive and negative effects, yet researchers typically focus on the negative aspects in order to examine ways to minimize interruptions and decrease the risk of error. More than one third of the interruptions were considered appropriate, indicating there is value to certain interruptions. Furthermore, the presence of interruption reveals there is system flexibility to make performance adjustments as necessary. The results suggest that appropriate interruptions assist the clinical team function in the ED by providing updates on patients and discussing care plans. The characteristics of the appropriate interruptions also indicate a lack of protocol for admitting patients when resources are limited. Future work will involve including clinicians in the process of identifying and understanding appropriate interruptions to facilitate resilience education in the ED setting. Additional work will investigate the 'negative' interruptions in order to evaluate the tasks and events that did go right.

STAff MEMBERS' CHATS IN A REFRESH ROOM AS A WAY OF KNOWLEDGE SHARING FOR MAINTAINING THE RESILIENCE OF SOCIO-TECHNICAL SYSTEMS

Hidenori Fujino [1], Motoki Urayama [2], Takayoshi Kitamura [3], Hirotake Ishii [2], Hiroshi Shimoda [2]

[1] Faculty of Economics, Fukui Prefectural University – 4-1-1, Matsuoka-Kenjojima, Eiheiji-cho, Yoshida-gun, Fukui, Japan

[2] Graduate school of Energy Science, Kyoto University – Japan

[3] College of Information Science and Engineering, Ritsumeikan University – Japan

fujino@fpu.ac.jp

For maintaining resilience of every socio-technical system, it is believed necessary to learn not only from unsafe events but also from normal operation [1]. To develop a safety information system figured by J. Reason [2] is an usual methodology for enhancing learning from unsafe events. However, it is often difficult to enhance learning from normal operation by this methodology caused on its nature of a safety information system. The most critical problem is that this system should be depending on information reported by staffs, while it would be difficult for them to find out information should be reported from their daily normal operation or figure out the information to a "report" (usually as a written paper) on their own. By the way, in a refresh room, many staffs usually chat lively about various topics, some of which are related to their jobs. Such a chat can include information to be learnt, like knowhow to mitigate a threat, a new idea to improve their performance as well as their experience of a previous incident or error, of course. Further, Chatting is believed an effective media to enhance learning from them because 1) they can use non-verbal language, onomatopoeia or various rhetoric like metaphor, to more lively and correctly express their intended information, 2) they can modify their expression to get intended information shared correctly with watching reactions of a companion, and 3) they can more clarify their own knowledge as they have a communication as a situated interaction, even if they wouldn't have had so clear image of the knowledge in them before chatting. Therefore, authors expect that enhancing lively chats can lead sharing some information which is difficult to be shared by Reason's safety management systems.

Standing on this background, authors conducted a survey to examine the relationship between chats in a refresh room and knowledge sharing about safety in a Japanese hospital. As a result, it was suggested that not only a frequency to participate in chats in a refresh room but also a frequency of their chat about their job (especially positive experience in jobs) would positively affect how much knowledge related to safety would be shared. Furthermore, authors attempted to develop a new method to enhance chats related to positive job experience applying Information Communication Technology and theories of cognitive psychology. As long as the laboratory experiments, the result showed that authors' method was effective to enhance a chat with a specific topic that authors intended to enhance.

The limitation and future work is discussed in a full paper and presentation. A part of this study was funded by West Japan Railway Company in 2014.

Hollnagel, E. and Woods, D.D. (2006). Epilogue: Resilience Engineering Precepts. In Hollnagel, E., Woods, D. and Leveson, N. Resilience Engineering : Concepts and Precepts (pp.346-358), Ashgate

J. T. Reason and A. Hobbs, Managing Maintenance Error: A Practical Guide. Ashgate, 2003.

Keywords: knowledge sharing, informal communication, chats in a refresh room, learning

DESIGN OF A FUNCTIONAL MODELING BASED TECHNIQUE TO SUPPORT OPERATORS ON IMPROVISING COUNTER-MEASURES FOR UNEXPECTED EVENTS

Song Mengchu [1], Gofuku Akio [1]

[1] Graduate school of Natural science and technology, Okayama University – Japan

song.m.mif@s.okayama-u.ac.jp

Lessons from the Fukushima disaster indicate that there is an inadequate response capability. Responding, the ability of knowing what to do and being able to do, is one of the key capabilities of resilience engineering. Strict compliance of procedures can indeed make the plant more resilient in responding to the accidents. The unexpected situations, however, are challenging to plan a response, when nothing has been prepared in advance. Operators are required to take advantage of available plant equipment and even their creativity to improvise a counter-measure to mitigate the accidents. In perspective of resilience engineering, it means the need of adapting functioning and matching the conditions to sustain desired goals during the unexpected. We must acknowledge that it is hard for human to handle these complex knowledge-based tasks even they have been well trained. This study therefore focuses on how adapting capability of operators in responding can be strengthened by technology. A computerized operator support system on human-machine interface is designed based on functional modeling of plant knowledge. With the influence propagation rules in a model, a series of operations on components to achieve a safety goal can be identified whether the plant conditions are expected or not. An example that is similar with the accident of Fukushima Daiichi nuclear power plants is used to demonstrate how the technique can generate multiple mitigation alternatives when various safety systems are unavailable and rare responses are prepared.

EXPLORING EfficACY OF ADAPTIVE SAFETY PRACTICE FOR SOCIAL SUSTAINABILITY IN CONSTRUCTION SUPPLY CHAIN MANAGEMENT

O'loughlin Maeve [1]

[1] Middlesex University London – The Burroughs, Hendon, London NW4 4BT, United Kingdom

The adaptive age of safety[i] is argued as transcending traditional safety practice through providing a different lens from which to consider organisational practices. The orientation towards acceptance of adaptive capabilities refocuses the view of workers as a source of innovation and a solution to safety performance[ii]. Centred on the 'messy' reality of work with variable demands, resources and trade-offs[iii]; questionable faith in prescribed systems, and understanding of the rational acts of workers, the blurred lines between facilitating productivity and safety make it a strategically attractive prospect for organisations in justifying the business case for safety management and reducing bureaucracy. In contrast to other industries who are applying these theories, the Construction Sector relies on temporary, dynamic and multi-stakeholder networks within a supply chain setting. Planning and delivery exist temporally and logistically remote to one another[iv]. Approaches to addressing adaptive safety require mechanisms for anticipating, monitoring, responding and learning about and from challenges in an effective manner that requires engagement and commitment underpinned by a just culture and safety leadership across the supply chain[v]. In this highly fragmented, transient sector, this can prove difficult.

Recently, there is some evidence in the public domain that companies within UK construction are turning away from 'zero accident vision', and the traditional foundation of compliance it embodies, to explore the potential for resilience through adaptive safety. Industry efforts are also evident to transform CDM management. With a strategic organisational change in ethos, employee-centric engagement processes, which include appreciative enquiry, collective insights and evaluation of normal work, are contributing to narrowing the gap between belief and reality in providing a key source of organisational learning for work effectiveness and safety. This is being examined as part of PhD research.

The overall PhD research aims to explore the efficacy of applying adaptive safety theory to construction supply chain management and the alignment of this theory to social sustainability principles at an supply chain level. Following initial theory construction with systematic combining using abductive logic, a small grant from the Supply Chain Sustainability School UK will soon fund a survey of construction industry orientation towards the 'new view' of safety. Case studies which differentiate varying procurement models and therefore construction supply chain dynamics will also be carried out. These efforts propose an outcome that shall support the construction sector more widely to evolve safety practice.

This proposal aims to provide details on the methods and initial findings from ongoing work on this project. It is proposed to deliver this outcome with a poster at REA2017.

i Borys, D., Else, D., & Leggett, S. (2009). The fifth age of safety: The adaptive age? Journal of Health and Safety Research and Practice, 1(1), 19–27

ii Dekker S. W. (2014b). Safety differently: Human factors for a new era. Boca Raton, FL: CRC Press

iii Hollnagel, E. (2009). The ETTO principle: Efficiency-Thoroughness Trade-Off. Why things that go right sometimes go wrong. Farnham, UK: Ashgate.

iv Holmes, N., Lingard, H., Yesilyurt, Z., & De Munk, F. (1999). An exploratory study of meanings of risk control for long term and acute effect occupational health and safety risks in small business construction firm. Journal of Safety Research, 30(4), 251-261.

v Hollnagel, E. Pari`es, J. Woods, D. D. & Wreathall, J. (Eds) (2011). Resilience Engineering Perspectives Volume 3: Resilience Engineering in Practice. Farnham, UK: Ashgate.

Keywords: adaptive safety, construction, supply chain, culture

RESILIENT CAPABILITIES IN SINGLE PILOT AND CREWED flIGHT OPERATIONS

Shawn Pruchnicki [2,1], Arjun Rao [1], Seth Young [1]

[1] The Ohio State University, Center for Aviation Studies – United States

[2] The Ohio State University, Department of Integrated Systems Engineering – United States

Pruchnicki.4@osu.edu

Pilots are increasingly encountering unexpected events (e.g., loss of control) for which they sometimes do not have procedures or specific checklists to consult. Unfortunately, some of these events deteriorate to aircraft upsets, loss of control, and other undesired aircraft states eventually resulting in both, successful and unsuccessful accidents. When faced with these events, pilots are expected to evaluate the operational circumstances and respond in an appropriate way; whether it is an aircraft malfunction, environmental threat, or other types of threats including combinations. Pilots are expected to be cognitively equipped to handle any possible threat experience. However, as past accidents have shown, both individual pilots and crews do not always perform equally well in all of these situations. Furthermore, research has shown that pilots who appear to be more resilient than others when faced with such events tend to have better outcomes [1]. Here, we present research that helps us better understand what resilient skills or strategies are most effective when faced with unexpected events. By reviewing past accidents and observing in real-time routine simulator proficiency checks, the types of resilient strategies that are deployed to make some accidents more successful than others (e.g., US Airways flight 1549 vs. American Airlines 587), or the determination of check ride pass/fail outcomes. After an extensive literature review across numerous domains, including aviation, we have identified those efforts described there as resilient skills, capabilities, and indicators.

The value of this research for the global community is in the identification of requisite resilient skills for problem solving/decision making when confronted with an unexpected event. We suggest that these skills, of which many are described in the aviation literature, are potentially deployable to other domains. To demonstrate their efficacy, we first extracted from the literature base, these resilient skills as demonstrated and observed across numerous safety-sensitive domains. We then searched for these resilient skills in those accidents that can be described as both successful and unsuccessful. Further, we proceeded to identify these same skills or strategies while observing both successful and unsuccessful check rides. Our goal is to verify if the resilient skills from literature appear in both historical accident reports, and real-time check rides (in flight simulators). From the earlier literature base review, to the accident reports and simulator observations, we envisage being able to decide on the resilient skills or strategies consistent throughout this research, and propose to construct a resilient training course for pilots that can now be tested empirically. To achieve our goal, we will design a simulator-training event where one group of pilots will be trained in these skills, while a second group (which will serve as our control group) will not receive resilient skills training. We aspire to show that those pilots that received resilient training perform better than those that did not as found in the literature base, accident reports and check-ride events.

Regardless of the safety-sensitive domain, those at the sharp end are challenged beyond capabilities when confronted with situations that are both unexpected and exceed the norms of what could be considered normal failures. These types of events are impossible to train for a priori because of their extreme and unique nature that make them only possible to grasp in concept after they occur. What this research offers in value across domains, not just aviation, is that if these resilient skills are shown to be effective when facing challenging unexpected events that stretch resilient capabilities beyond what could be described as normally trained for expected technical events, then these additional capabilities can now be deployed to help ensure success. Essentially, we will have shown that resilient skills training is effective and positions those at the sharp end with additional skills that can be deployed when facing events that are both unexpected and that exceed the typical technical events for which they are already proficiently trained.

Dekker, S. W., & Lundstrom, J. (2006). From threat and error management (TEM) to resilience. Human Factors and Aerospace Safety, 6(3), 261.

CITY RESILIENCE: ANALYSIS OF STRATEGIES WORLD-WIDE

Amy Rankin [1], René Lindner, Maider Sainz, Simon Rosenqvist, Magnus Bang, Henrik Eriksson

[1] Department of Computer and Information Science - Link¨oping University – SE-581 83 LINK¨OPING SWEDEN, Sweden Corresponding author: amy.rankin@liu.se

Increasing resilience to crises and disasters is a topic of highest political concern worldwide. Cities and communities need methods and tools to prevent and manage the effects of natural hazards such as floods, storms, earthquakes, and tsunamis as well as man-made threats such as accidents and terrorism. A challenge when developing such methods and tools is to go from theory to practice, that is, from theoretical models of resilience to methods for applications and concrete action plans. The 100 Resilient Cities [1] (100RC) initiative, founded by the Rockefeller Foundation, is a global initiative to support and improve resilience at the community-level. In this paper, we analyze 18 RC100 member cities and their resilience strategies. The aim of the analysis is to identify common challenges and suggested actions to improve city resilience. Also, the analysis aims to highlight differences and commonalities with regards to resilience implementation processes, offering a discussion on the generalisability of the approaches. Furthermore, a set of interviews with city representatives in the Smart Mature Resilience (SMR) project [2] are carried out regarding implementation of 100RC strategies and SMR resilience strategies.

The results of the study indicate that the resilience strategies and concrete actions of the 100RC cities are focused on measures to improve community cohesion and information gathering (monitoring), and resilience-thinking based on graceful management of ”disasters” (e.g., being in control of a flood). With regards to cohesion, cities aim to approach internal management silos as well as improving communication with citizens, business and other stakeholders. A common approach to tackle challenges identified by the 100RC cities include creating community plans and expanding present programs or plans. A widely-applied solution is to modify evaluation processes of already existing projects to also include aspects of resilience, with the aim to make it an integral part of policy-making and everyday operations. However, approaches to manage the local challenges vary greatly between cities, and are adapted to local possibilities and constraints such as the cities ecology, geology and history. The latter indicates that resilience guidelines and tools must allow local contextualization. The findings of the study offer insights for (1) the development of support tools to aid the resilience building process in general and, (2) the replication efforts, the standardization potentials and the practical uptake of developing and implementing City Resilience Strategies within the 100RC framework.

SIGNIFICANCE/TAKEAWAY : Theories of resilience have in the past decade developed models and methods to understand resilience, demonstrating the importance of resilience to cope with complex and dynamic events such as crises and disasters. However, critical questions on how to operationalize resilience are still unanswered and more examples of applying resilience concepts to real-world problems is needed. In this paper we explore the development and content of city action plans (strategies) aimed at increasing city resilience. The paper discusses hand-on practical applications that aim to increase city resilience, offering guidance to (1) development of support tools, and (2) city representatives aiming to set up an action plan for city resilience.

http://www.100resilientcities.org/

http://smr-project.eu/home/home/

Keywords: City, Community, Resilience, Strategies, Action plan

A DECISION SUPPORT FRAMEWORK FOR IMPROVING CROSS-BORDER AREA RESILIENCE TO DISASTERS

Eric Rigaud [1]

[1] MINES ParisTech, PSL Research University, CRC, Centre de recherche sur les risques et les crises (CRC) – MINES ParisTech - ´Ecole nationale sup´erieure des mines de Paris – CS 10207 rue Claude Daunesse 06904 Sophia Antipolis Cedex, France, France

In spring 2017 the research-project INCA (A Decision Support Framework for Improving Cross-border Area Resilience to Disasters) with a French-German consortium will start. Aim of the proposal is to presents the context, the aims, the methodology and the results expected of the project. The aim of the INCA project is to contribute to the understanding and to the enhancing of cross-border area resilience with regard to the risk of disasters by considering two topics in particular: the resilience of medical dependent citizens and the management of volunteers in a cross-border area. Scientific knowledge and decision-makers' contributions to cross border areas resilience to disasters will be enhanced with an interdisciplinary approach combining conceptual and empirical research, decision support system engineering and a campaign of experiments. Results of the project will be novel models for the thematic of cross border area resilience and on the perspective of medical dependent citizens and volunteers; an assessment tool; a set of experiments rapports on the utility, usability and acceptability of the solution developed and practical experience for resilience to disaster stakeholders.

Keywords: Disaster Resilience, Cross border, Black out, decision support system

VOLUNTARY SAFETY LEADER AT THE SHARP-END: FROM CONTROLLED SAFETY TO CREATIVE SAFETY AT AN EXPRESSWAY MAINTENANCE SITE

Masayoshi Shigemori [1], Remi Ohshima [2], Shigeru Haga [2]

[1] Shizuoka Eiwa Gakuin University Junior College – Japan

[2] Rikkyo University – Japan

Background Now that we have identified the limits of the SAFETY-I or controlled safety model[i] which requires making and following a comprehensive safety manual, our next objective is creative safety, which requires flexible and creative correspondence regarding unexpected situations and efficient requirements on site[ii]. Creative safety also aims for resilience on site. Creative safety is not so straight forward, however, as simply requiring workers at the sharp end of a situation to make decisions flexibly and think creatively, as there may be a wide variation in individual workers' ability to do so. To accumulate the information, we will need to resolve this difficulty; the authors interviewed site workers, most of whom are employed by an expressway maintenance company. The results indicated a need for specific safety workers who volunteer to pay particular attention to unexpected dangers or dangers caused by efficiency requirements and to cope with these dangers as they unfold. We call these workers the voluntary safety leaders and have written this study with the aim of clarifying their necessary attributes.

Methods: We developed the safety leader index, a 69-items questionnaire based on the developed leadership scales[iii],[iv]. We asked 440 site workers at an expressway maintenance company to complete this questionnaire, once with their safety manager in mind and a second time with their voluntary safety leader, if they had one, in mind. The safety manager is a position assigned by the company; for the voluntary safety leader, we asked workers to think of one of their colleagues who, although not assigned a safety-oriented role by the company, took particular care for workers' safety. Finally, we asked them to answer 11 questions regarding the workplace safety climate.

Results: We received intact data from 101 out of 440 participants. We received completed questionnaires regarding both safety leaders from 59 participants. We compared the two leader types' average scores for each item through a T test. On 16 of the 69 items, the voluntary safety leaders received higher scores than the safety managers did. We performed factor analysis on these 16 items for the 101 participants. The results indicated two factors, which we named ”troubleshooting” and ”commitment to colleagues.” We then performed multiple regression analysis dependent on workplace safety attitude as assessed by means of the final 11 items. Only ”commitment to colleagues” contributed to workplace safety attitude. Therefore, we concluded that the seven items associated with ”commitment to colleagues” represented the necessary attributes of a voluntary safety leader. According to these seven items, a voluntary safety leader involved in work allocation, information delivery, and operational instruction; is able to think for his/her colleagues in a dangerous situation; and consistently emphasizes safety.

Discussion : Our study identified the necessary attributes of a voluntary safety leader at the sharp end. Being aware of these attributes, and, in the future, identifying the environmental factors that produce leaders with these attributes will enable us to develop ways to train such leaders and thus to realize more resilient organizations.

Keywords: leadership, safety, flexibility, creativity, organizational safety

ASSESSING RESILIENCE THROUGH INVESTIGATING ADAPTIVE CAPACITY

Anthony Smoker [1], Matthieu Branlat [2], Ivonne Herrera [3], Rogier Woltjer [4], Billy Josefsson [5]

[1] Lunds Universitet, Division of Risk Management and Societal, Sweden (LTH) – Lund University Box 118 22100 LUND, Sweden

[2] SINTEF – Norway

[3] SINTEF (SINTEF) – Norway

[4] FOI – Sweden 5 LFV – Sweden

Matthieu.Branlat@sintef.no

While numerous definitions of resilience exist, the field of Resilience Engineering puts the notion of adaptive capacity at the centre of its investigation of work systems. Given the nature of most operational environments, especially in typical high-risk, high-consequence domains, adaptive capacity is understood in the context of complexity, uncertainty and variability. Resilience Engineering is primarily concerned with how work systems adapt to challenging events and surprises; that typically characterise adaptations to compensate for performance variability influences system performance. Exploring adaptive capacity, in unusual events as well as in everyday operations, thereby provides the means to explore resilient performance. New designs or concepts of operation transform the work, changing the requirements and capabilities for adaptation, thus changing the nature of resilient performance. In some instances, the sources of resilience that facilitate resilient performance can change. The introduction of new ways of conducting work can lead to the unintended consequences of creating new forms of brittleness in the work system. In other cases, the work system can be juxtaposed to another work system undertaking an adaptation, and experiences a demand upon its own sources of resilience that can induce brittleness] The notion of graceful extensibility has been proposed to capture how a system exhibits resilience by successfully adapting at or beyond its typical boundaries of operation. When new designs or concepts of operation change the sources of resilience and brittleness, they impact graceful extensibility as well.

In one project to operationalise RE, the application of an Resilience Engineering method built on eight principles of resilience to explore work-as done and work as envisaged, encountered a number of methodological issues. Alternative ways of operationalising RE were considered and a focus on adaptive capacity was deemed to be a more productive way to explore the nature of resilient performance. Woods and Wears (2013) adopts a 'stress strain' approach to adaptive capacity. This model, plots the adaptive landscape by representing the base and extra adaptive capacity of a work system. The Woods & Wears model was used in one approach to operationalise RE and in particular to explore and identify adaptive shortfalls between current operations and a new system design. In particular can shortfalls in the adaptive landscape be identified and how would this be identified. Responses to performance variability frequently involve building strategies that draw upon sources of resilience that access a work systems adaptive capacity. Such strategies involve a subtle interplay of managing the system through its sources of resilience. There are consequences and costs associated with these e.g. the costs of coordination and collaboration that will follow as a result of the strategies used. Understanding these provides the knowledge by which to explore a socio-technical systems adaptive capacity and resilient performance.

The paper discusses the theoretical issues around adaptive capacity, graceful extensibility and brittleness the implications for real world application to achieve resilient performance in an Air Traffic Management concept development, and the implications for Resilience Engineering

Keywords: Adaptive Capacity, Adaptive landscape, work systems, adaptations, sources of resilience, works done

THE RELATIONSHIP BETWEEN LEAN PRODUCTION AND THE COMPLEXITY OF SOCIO-TECHNICAL SYSTEMS

Marlon Soliman [1], Tarcisio Saurin [1]

[1] Industrial Engineering Department. Federal University of Rio Grande do Sul – Brazil

The need of companies to increase productive efficiency has been paying attention to the issue of lean production since the 1990s. However, the increasing organizational complexity is evident today, so that production systems are more connected and subject to the unpredictability and dynamism of the external environment. In this sense, recent studies indicate that complexity is responsible for restricting the advance of lean practices. However, these studies are not supported by complexity theory, which is inconsistent, since complexity may also play an important role in sustaining PE. Thus, the research presented in this doctoral thesis aims to characterize and evaluate the impacts of lean production on the complexity of socio-technical systems, using methods aligned with complexity theory. The research strategy was divided into three stages: exploratory research; descriptive; and explanatory. In the first phase, a systematic review of the literature was conducted to show the state of the art in relation to the theme and the existing knowledge gaps. Afterwards, a study in the form of a survey sought to characterize how companies with a higher level of lean principles adoption differ from others in relation to the complexity of their systems. Finally, the explanatory step sought through a case study to model the dynamics involved that support PE in a complex system. At the end of this research, it is expected as an academic contribution to present an in-depth understanding of how PE relates to organizational complexity, as well as to propose guidelines that assist in lean implementation in complex systems, taking into account the distinct nature of these systems.

Keywords: Lean production, Complexity, Complex systems, Socio, technical systems

THE GAP BETWEEN WORK-AS-IMAGINED AND WORK-AS-DONE AS AN INDICATION FOR SAFETY

Kaspers Steffen [1]

[1] Aviation Academy, Amsterdam University of Applied Sciences – Netherlands

Safety is imperative for operations within aviation. Many companies try to measure their level of safety but acknowledge that it is very hard to do in everyday practice. Therefore, new indicators are necessary. This poster explains how the gap between Work-as-Imagined (WaI) and Work-as-Done (WaD) is explored to be a better indicator for safety with the help of agent based modelling. Current safety indicators have severe limitations. There are process and outcome metrics and most safety indicators are based on outcomes with unclear thresholds. Scarce evidence between the relation of process metrics and safety outcomes exists, and therefore the relation is based on credible reasoning. Most of the safety models used in the industry are linear and therefore not representative of current complexity of their operations. The gap between WaI and WaD is a promising indicator according to the literature and practice. Recent literature suggests that the gap between work realities affects safety and the industry already explores the gap. Agent based modelling will be used to create two models, one of WaI and one of WaD which can be compared with the help of a distance vector. Sensitivity analysis will help identify the 'parameters' which will influence the process, outcomes and safety the most.

ORGANISATIONAL INTERDEPENDENCIES AND EMERGENCY RESPONSE

Justyna Tasic [1]

[1] Nanyang Technological University; Future Resilient Systems Programme, Singapore-ETH Centre (NTU; FRS) – Singapore

This study addresses the major challenge of understanding the organizational structure of sociotechnical systems. Organisational behaviour-human decisions, routines, and actionstremendously affects system safety and capacity to recover from disruptions. However, human interactions within a complex sociotechnical organization are hard to detect and measure, and cannot be described by a linear model. In this study, the organisational structure is examined from a multi-layered perspective. More specifically, the structure is analysed as social networks embedded in the specific sociotechnical context. Thus, to investigate organisational interdependencies, the research focus embraces both formal and informal organisational structure seen as multi-layered networks of actors. This study aims to identify and measure the degree of organisational interdependencies and develops a multilayer model of organisational system to locate fault-prone and fault-tolerant interactions. By identifying vulnerabilities within the structure of organisational interdependencies, this study seeks to provide new insights on the consequences of organisational interdependencies on system resilience. Additionally, the analysis of fault-tolerant areas allows indicating good practices and guidelines for proactive management and anticipation of risk to enhance organisational capacity in coping with disruption and crisis.

Keywords: organisational interdependencies, organisational resilience, crisis, sociotechnical system.

BUILDING AN ”ADAPTIVE SAFETY CULTURE” IN A NUCLEAR CONSTRUCTION PROJECT – INSIGHTS TO SAFETY PRACTITIONERS

Kaupo Viitanen [1], Teemu Reiman [2]

[1] VTT Technical Research Centre of Finland – Finland

[2] Fennovoima Oy – Finland

Safety practitioners are in a central role in creating the preconditions and direction for the development of a shared safety culture in high-risk organizations. The work of safety practitioners has been approached from leadership and managerial perspectives. It has been proposed that safety practitioners require both approaches to be successful. The dynamic project environment creates extra challenges for the creation of strong safety culture. Change is constant due to e.g. growth of personnel at the participating companies, changes in the phase of the project, various unanticipated occurrences, multiple interacting parties and multicultural environment. All this puts increased emphasis on safety practitioners in creating and maintaining the foundations (incl. working practices, cultural values and assumptions) upon which performance in the nuclear project should be based on.

Basing on previous research, Reiman et al. have proposed an adaptive model of safety management which identifies four tensions, each consisting of a conflicting pair of management goals: 1) system goals – local goals 2) repeatability and systematic response - flexibility and adaptability, 3) low system variance – high system variance, and 4) few strong ties – multiple weak ties. We will examine the implications of the model from the perspective of a set of practical safety culture improvement methods. The model suggests that safety practitioners need to be able to recognize and manage the tensions adaptively, depending on the context. It further means they need to use different methods depending on a variety of factors in their organization and its environment.

Our objective is to shed light on how the conflicting management principles can manifest themselves in the concrete activities of safety practitioners, highlight the paradoxical nature of these programmatic methods of changing complex adaptive systems and to provide insight for practitioners on how to manage these issues. Four approaches to safety culture improvement were chosen based on the authors' previous experience: Safety training, Behaviour modification programs, Safety culture auditing, Facilitation of employee involvement and participation. The first author has conducted research and consultancy work related to these methods, and the second author has first-hand experience in applying these methods as a safety culture manager in a large nuclear power plant construction project.

In this paper we will view safety leadership and management from the perspective of resilience engineering and complexity thinking and present a novel perspective to the practical development of safety culture in dynamic environments. Our focus will especially be on the role of safety practitioners, who typically hold either an expert or a middle management position. The key question is about adaptation between the inherent properties of different methods (e.g. training), the constrains and possibilities of their utilization (e.g. choice of training approach and topics), the current phase of the organization in terms of work activities, and the current 'level' of safety culture (including attitudes towards training). We will present needed corrections to the model in order to accommodate findings from the application of the model in a nuclear power plant construction project.

Keywords: safety culture, safety management, safety leadership, nuclear safety

DEVELOPING AVIATION ORGANISATIONS' AGILE RESPONSE CAPABILITY

Rogier Woltje[1], Björn Johansson, Peter Svenmarck, Per-Anders Oskarsson

[1] Swedish Defence Research Agency (FOI) – Sweden

rogier.woltjer@foi.se

Aviation is a highly inter-connected system of systems. This means that a problem in one area may not be confined to the local system. Instead it may cause effects in other countries or parts of the Air Transport System (ATS), for example a fire in an airport area may lead to the shutdown of the airport, and if it is a major hub, this can cause disruption over a large part of Europe. Additionally, there is the potential for massive system-wide events such as the volcanic ash crisis. The immediate response to the first volcanic ash crisis was uncoordinated and could even be called chaotic. The possibility of ”man-made” accidental events as well as intentional coordinated events must increasingly be taken into account. The resulting approach of Future Sky Safety WP5.4 (2,3) combining Agility and Resilience Engineering perspectives is to provide aviation organisations with an Agile Response Capability (ARC). This poster aims to present work-in-progress on the development of the ARC approach. Two important aspects to be explored according to agility research are here called the problem space, or the parameters that play an important role in developing and applying an appropriate response, and the solution space, or the parameters that can be varied in the organization of the response in terms of information dissemination, allocation of decision rights and interactions within the response organisation. Guiding questions to explore these spaces are presented. As an illustration of its applicability the poster applies the essential questions of the ARC approach on a literature survey on the first volcanic ash crisis, which by now is quite welldocumented in industry reports and scientific publications. 27 documents and publications were analysed for the literature review. The application of the ARC approach explores the problem space of Eyjafjallaj´’okull ash cloud crisis in 2010, and then explores what the documents analysed reveal on the solution space of how aviation organisations individually and jointly endeavoured to meet the crisis. Implications for how aviation organisations could exercise their agility using ARC guidance are provided.

Keywords: agility, resilience, aviation, crisis response, crisis exercises, volcanic ash

Workshops’ Proposals

OPERATIONALIZING RESILIENCE THROUGH RESILIENCE MANAGEMENT GUIDELINES

Matthieu Branlat [1], Ivonne Herrera[1], Luca Save[2], Sabina Giorgi [3], Luca Rosi[3], Valentina Cedrini

[1] SINTEF – Norway

[2] Deep Blue srl – Italy

[3] Istituto Superiore di Sanità – Italy

[4] ENAV – Italy

Matthieu.Branlat@sintef.no

Background information Crises are typical situations for which the concept of resilience is highly relevant (and has undoubtedly grown in popularity). Faced with the limited predictability and increased complexity of crises, organisations operating critical infrastructures, would like to develop and enhance capabilities to sustain operations and services through, for instance: broadening knowledge in personnel at different levels of the organisations to foster flexibility and better compensate for the potential gaps in plans and procedures; increasing teamwork and effectively coordinating across organisations involved in crises; better including communities as stakeholders and potential actors of crisis management. Such capabilities are well in line with the theories and concepts developed in the research fields of Resilience Engineering and Community Resilience. However, the operationalization of these resilience concepts is still difficult and limited. This challenge is addressed by Horizon 2020 project DARWIN, which aims to build resilience management guidelines to support organisations in developing and enhancing their resilience in the context of crisis management. In this project, we work with the development of practical guidelines based on concepts, practices, methods and tools associated with the Resilience Engineering and Community Resilience areas of research. The context is that of organisations that already have a number of processes and tools in place to support their management of crises (e.g., preparation activities, contingency plans, procedures, learning activities). The guidelines are positioned at a meta-level: they provide a perspective on these processes and tools grounded in research and practice on resilience management. The guidelines propose interventions that can be implemented to enhance resilience capabilities and complement existing crisis management processes and practices. The information provided aims to support the understanding and implementation of the interventions proposed, as well as to help users adopt a resilience-oriented perspective, which might differ from typical views on risk and safety. The interventions often refer to strategies, methods, tools and practices that are selected from literature or experience, and presented succinctly.

Objectives and format: Based on an overview of the DARWIN project, the workshop aims to introduce participants to the guidelines developed and discuss their applicability to their respective work domains and organisations. The workshop will address generic as well as specific considerations: project members will share their experiences with the adaptation of the guidelines to the domains of Healthcare and Air Traffic Management in order to as well as foster generalisation across domains. The DARWIN project will enter its last year at the time of the symposium; the workshop will therefore be an opportunity to gather expert feedback and make appropriate changes.

Duration: The proposed workshop would be organised over half a day. We plan to minimise presentation time and rely on various activities to support interactions with participants. The activities will serve to explore with participants the content of the guidelines, imagine the use(s) of the guidelines and gather feedback on their added value for the management of resilience, especially related to crisis situations.

Participants: Target audience includes, but is not restricted to, designers, practitioners, operators, managers and regulators from different domains (e.g., nuclear, energy, transportation, construction). Participants envisioned would provide a balance between regulators, researchers, operators, maintenance personnel, managers.

About the workshop organisers Organisers of the workshop represent a balanced mix of applied research, consulting and practice, allowing for fruitful discussions allowing for the transition from theory to practical solutions.

WORKSHOP: ONE BEST METHOD, DOES IT EXIST? NO!

Ruud Plomb [1], Jurriaan Cals [1]

[1] Artemas BV – Netherlands

jurriaan@artemas.eu

Summary of the proposal Workshop: One best method, does it exist? NO!

The workshop is an introduction of the Rhineland philosophy in Safety. We designed an interactive exchange with participants.

What kind of resilience does 2017 and further need?

We think we know the answer, we think we can foretell what the possible future brings and what workers need to do in order to be able adapt to that expected reality. But do we really?

NO we don't. The future brings us always something that is or will be more or less unexpected, even without the "black swans" included. Off course we would like to know, and even to be sure about what's going to happen in order to control it and to be able to prepare for it. If this would be possible then we would be able to board up rules and regulations. The problem for the modernist managers and safety professionals is that real life does not comply with their beliefs. However great their desire may be, we are not able to create or predict the future.

Over the last decades we have (slowly) built safety systems that are based on the modernist belief of a known future. Among those all kind of behaviour based safety programs that are mainly introduced to control the employees at the sharp end. We have tamed our employees to do what is conceived. Conceived by the former generation and managers that have lost the connection/feeling with the workforce and reality. And we have tamed the employees to follow what we say not what their brain tells them to do. We have made them to pawns of a game we invented. We didn't reward them for establishing craftsmanship, we reward them for following instructions, or even worse, we blame them when they don't follow them.

Total control from above was our goal. Control over the environment, over people's work, which was achieved by imposing control hierarchically. This is modernism. It wants to improve the world by making things more rational and more technical, by making them less haphazard and less improvised. By deleting their improvisation qualities. We have made them dumber than they were when they started. This should keep us awake at night!

So what's next? How do we build resilient organisations using the Rhinish filosophy? First by understanding the reason why we didn't so far. We have created an Anglo Saxon illusion or an air bubble. On paper we have taken care of everything. For every event we have a solid rule, procedure or guideline, in the assumption that we are able to be prepare for (almost) everything.

1) Safety Differently, Sidney Dekker

Whether an organisation is resilient,is depending on the 'quality' of the people of that organisation. They determine the quality of what is going on. We call it the Rhinish way of organising. It's not command, control, communication and intelligence that should lead the company, the Rhinish assumptions are craftsmanship, connection, trust and inspiration. Not CCCI but CCTI. Rule based versus principle based. Employees have to carry out "orders" versus "Employees carry out assignments" In this workshop we are going to explore how safety could be embedded in the Rhinish operating system of an organisation. The participants are being challenged to use the Rhineland perspective to determine a different approach to safety. An approach that doesn't see 'sharp end workers' as the problem to control. But instead, they are seen as the most important key players who are able to effectively respond to unforeseen developments.

HOW CAN SAFETY PROFESSIONALS IMPROVE THE RESILIENCE OF THEIR ORGANISATIONS?

David Provan [1], Sidney Dekker [1], Andrew Rae [1]

[1] Griffith University – Australia

david.provan@griffithuni.edu.au

Over the past 25 years, we have continuously developed our theoretical and practical understanding of resilience within organizations. However, a comprehensive literature review of safety professionals over this period reveals that the design and practice of their role is steeped in the current paradigm and traditional safety thinking. The tasks, behaviors, and capabilities of safety professionals are presumed to influence the safety and resilience of organizations, and re-designing this role is a practical early step that can be taken to improve resilience. The language, activities, and capabilities of the safety profession need to change to create a role that facilitates the outcomes described in the resilience engineering literature. There is currently, however, little practical direction on how to re-design a safety professional's role to enable a resilience approach. Following the Columbia Space Shuttle incident, Woods (2006) described the 4 I's of a safety organization as involved, informed, informative and independent, which provides a useful starting point for continuing the discussion ten years later. Our current research at Griffith University offers new insight into Safety Professionals' identity and practice – who they are, what they believe about safety, and how they think about their role. The aim of this workshop is to facilitate a discussion amongst attendees on how this role could and should be redesigned, including role title, objectives, responsibilities, authorities, capabilities, performance measurement, and professional development.

Keywords: Safety Professional, Resilience

SMALL DETAILS – BIG DIFFERENCE: CAN RESILIENCE DEVELOPMENT CHANGE THE FUTURE OF AVIATION?

Gunnar Steinhardt [1], Marc Frank [2]

[1] Cargolux Airlines International – Luxembourg Airport, 2990 Luxembourg, Luxembourg

[2] Luxair Luxembourg Airlines – Luxembourg Airport, 2987 Luxembourg, Luxembourg

marc.frank@luxairgroup.lu

Workshop proposal: In recent years, a new ghost emerged within the aviation industry. Training Managers and Operational Directors were whispering the name: Resilience Engineering. Was this the breakthrough we were so long waiting for? Was this the milestone to bring aviation safety to a new level? Very often the charm of scientific novelty is huge, however, the problem is to convey this new way of thinking to the front line practitioners in high risk environment. Without their support and commitment, every effort, no matter how noble, would be fruitless. The scientific results have to be transposed to the real world. Luxair Luxembourg Airlines was one of the first airlines in Europe to implement the concept of 'Resilience Engineering' within its Crew Resource Management (CRM) training programs for Flight and Cabin Crews. 'Resilience Development' has been made mandatory by the European Aviation Safety Agency (EASA, 2015) for Flight and Cabin Crews as of October 1st 2016. Since many airlines do not have the know-how to implement this concept, Luxair has decided to share its knowledge with the aviation world. After providing insight into the training content and methods used, the authors will use an aviation accident to illustrate how the principles of 'Resilience Engineering' would have had the potential to avoid this accident at several stages.

Keywords: Resilience Engineering, Resilience Development, Training, Safety

WORKSHOP AND DEMO TRAINING FOR OPERATIONAL RESILIENCE CAPABILITIES, A WORLD TO WIN

Johan Van Der Vorm [1], Kees Van Der Blom , John Van Schie, Tor Olav Grotan, Dolf Van Der Beek, Dianka Zuiderwijk, Luigi Macchi, Christiaan Poll

[1] AdviSafe Risk Management (ASRM) – Koperslagersweg 23, 1786 RA Den Helder, Netherlands

johanvandervorm@kpnmail.nl, kees.vanderblom@strukton.com

The reality of operations does not always follow the book. Operational circumstances may develop into surprising situations that procedures have not accounted for. Still, we make things work. Resilient performance recognizes surprise early and acts upon it through adaptation, which is critical for an organization to succeed. It enables continued safe operations under changing circumstances in everyday or crisis situations by creating innovative ways to deal with progressively changing circumstances. As operational situations become increasingly complex and interconnected, the predictability of disruptions decreases. Consequently, resilience capability becomes more relevant to cope with unexpected situations. Achieving that requires a seamless understanding throughout the organization and the organization's leadership team about what resilience means. Because of its implicit nature, resilience capability has not yet become part of organizational learning. TORC (Training for Operational Resilience Capabilities) aims to provide an innovative training for operational teams and management to recognize and facilitate resilience as a critical capability and take it out of the shadows of compliance. The training introduces the concept of operational resilience and guides you through the training and the TORC game, and it serves as a reference while the organization is maturing these concepts in day-to-day practice. This game has been developed in the SAFERA-program and has been applied successfully at the Dutch companies and expands is use in the Netherlands.

The TORC-consortium comprising TNO, D´edale en SINTEF together with the Dutch companies NAM, Strukton Rail and Infraspeed Maintenance BV have developed the TORC-training including a serious game on simulating real life cases of everyday industry operations. Both the consortium partners together with AdviSafe and VU University propose to offer a workshop demonstrating the development and the results of the serious game which is aimed at both field staff, management and integrated training.

During the workshop the genesis of the TORC game and the set up will be presented, experience in railroad and oil and gas industry be reported and the elements for a successful application of resilience be explained. A short demo invites participant of the workshop to experience the dynamics of the game and its potential.

In addition to the workshop core elements of the demo can be repeated as a Tableau vivant (a living poster) in parallel to the plenary of the symposium. This allows a broader audience to experience how resilience dynamics and practices can be trained successfully alongside the symposium program.

By presenting this dual set up the symposium will express the potential for serious gaming in preparing for resilience to its audience.

The Workshop organisers and their afiliations will be specified in a later stage: Johan van der Vorm, AdviSafe Risk Management and contact person; Kees van der Blom, Strukton Rail Tor Olav Grotan, SINTEF; Luigi Macchi, D´edale; Dolf van der Beek, TNO; John van Schie, NAM; Christiaan Poll, Infraspeed Maintenance BV; Dianka Zuiderwijk, VU Amsterdam, Department of Organization Sciences

Keywords: resilience, training, serious game, resilience capability, industry, fieldstaf, management, operations