PROCEEDINGS

Edited by
Pedro Ferreira, Johan van der Vorm and David Woods

Resilience Engineering Association: http://www.resilience-engineering-association.org
Download from the Resilience Engineering Association website/resources page: http://www.resilience-engineering-association.org/resources/

PROCEEDINGS

6TH SYMPOSIUM ON RESILIENCE ENGINEERING

Managing resilience, learning to be adaptable and proactive in an unpredictable world

22th- 25th June 2015 at Lisbon, Portugal

Welcome again

It was a privilege to host the 6th Symposium on resilience engineering in Lisbon, particularly at a time when the idea of resilience has become almost as appealing for all industry domains as Lisbon for tourism. Regardless of its appeal, the full extent of implications and potential benefits of resilience remains difficult to grasp. The resilience engineering community actively pursues this endeavour, aiming to address the wide range of challenges posed by variability and uncertainty. This perspective on resilience recognises foremost that such challenges have repercussions for complex system that greatly exceed the focus of risk management. It has evolved from the analysis of high complexity problems across many different industry domains and has not limited itself to any context or to types of events. Over the period of some 10 years, resilience engineering has become well established as a scientific community that spans across all regions of the world, and as a high value tool within many different industry domains. In the tradition of previous editions, the Lisbon symposium brought this community together once more under the spirit of mind inquisitive and diversified discussion.

Pedro Ferreira, Chairman of the Organising Committee and host of the 6th REA Symposium

August 2016

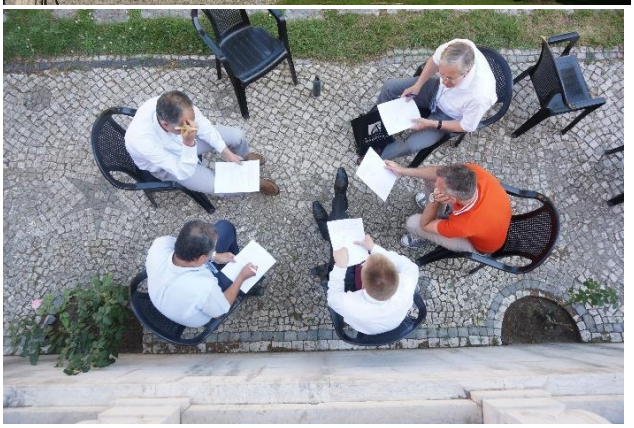


Fig. I, ISG building, symposium venue Lisbon

Fig. II, Workshop going on

Fig. III, Young Talents meeting

Fig. IV Jean Pariès Chairman of REA

Fig. V, Eric Hollnagel, Member of honour REA

Fig. VI, Symposium in action

Fig. VII, Fado group playing traditional Lisbon Fado at a perfect summer evening

Fig. VIII, Industry panel chaired by Jean Pariès

Fig. IX, Pedro Ferreira, Host of 6th REA symposium

Fig. X, David Woods, Chairman symposium

Fig. XI, ISG Garden, meeting and enjoying Portugese sun

Fig. XII, Anne-Sophie Nyssen, participating (Host of 7th REA symposium)

Colophon

Published by	Resilience Engineering Association
Editors	Pedro Ferreira, Johan van der Vorm and David Woods
Referents	Chris Nemeth and John Stoop
Publisher	Resilience Engineering Association, Sophia Antipolis Cedex, France. http://www.resilience-engineering-association.org/
Full title	Proceedings 6th Symposium on Resilience Engineering, Managing resilience, learning to be adaptable and proactive in an unpredictable world, 22nd -25th June 2015 at Lisbon, Portugal
Editing date	August 2016, version
Available at	Download from the Resilience Engineering Association website/resources page: http://www.resilience-engineering-association.org/resources/

Programming and Organizing committees

The Resilience Engineering Association acknowledges the following people for their contributions:

- The Programming committee: Ivonne Herrera, Pedro Fereira (vice chair).Erik Hollnagel, Jean Paries, Johan van der Vorm; and David Woods (chair)
- The Organizing committee: Arthur Dijkstra, Eric Rigaud,Pedro Ferreira (chair) Johan van der Vorm (vice-chair) and Dolf van der Beek and Matthieu Branlat (both Young Talent program).

Preface

Pursuing a tradition of open discussion and interactive participation, the 6th Resilience Engineering Symposium provided participants with an improved understanding of the strategies and resources needed to be adaptive and proactive in an unpredictable world. Among many highlights, David Mendonça led off a session on community resilience that began with the rise of risk management following Lisbon earthquake of 1755, continued with a number of contributions on the theme of community resilience, and ended with a general discussion of future directions (moderated by Michael Bruno, who has worked with Lloyds on this topic).

Another highlight was a session kicked off by Zoran Perkov, Chief Technology Officer at the IEX stock exchange, and John Allspaw, Senior Vice-President at Etsy, on resilience in business critical web operations. Business continuity and the financial sector are areas of growing interest for resilience. Zoran has created and runs the software that powers several stock exchanges and was part of the story of high frequency trading described in the book *Flash Boys: A Wall Street Revolt*. John uses resilience engineering principles to run the digital services at Etsy. Following a series of contributions, Richard Cook and Jan Maarten Schraagen kicked-off a general discussion of the opportunities in this area. But all these moments did not overshadow the many other contributions, discussions, and activities, such as the Industry Panel or the Young Talent Program.

Jean Pariès, Chairman of the Resilience Engineering Council on behalf of David Woods, Chairman of Symposium Programming Commmittee

August, 2016

Contents

The REA thanks its sponsors

Papers and abstracts

MANAGING RESILIENCE

TRAINING FOR OPERATIONAL RESILIENCE CAPABILITIES

Tor Olav Grøtan1 (corresponding author) and Johan van der Vorm2
1 SINTEF Technology and Society, Trondheim, Norway
tor.o.grotan@sintef.no +47 92039327
2 Netherlands Organisation of Applied Research, TNO
Leiden, Netherlands
johan.vandervorm@tno.nl;

Abstract

Based on the SAF€RA[1] project *Training for Operational Resilience Capabilities* (TORC), this paper describes a conceptual approach to operational and managerial training of resilience. The project aim is to develop a generic training program that constitutes generic *capabilities of resilient functioning in the context of a compliance-oriented safety regime*. Hence, TORC aims to develop an innovative training concept that enables organizations to appreciate, nurture and improve their inherent resilient and adaptive capacities, while being under the imperative of predominantly compliance-oriented safety regulations and standards. Training is addressed both at the operational and managerial level, including guidance for the calibration of such a training program in order to adapt it to the specific organizational context (history, aspiration, constraints, etc.). The overall initial framework and thinking (rationale, objectives, training philosophy etc.) as well as key concepts will be described, aiming for a parallel piloting activity in different industries and European countries. The methodological approach, including the concept and framework development based on the pilot projects, will be discussed, as well as the potential contribution to the understanding of Resilience Engineering.

1 INTRODUCTION

Successful adaptation to surprise and complexity is a situated practice that cannot be expected to recur in the exact same way. Resilience in organizations is an ability that benefits from training and rehearsal, but there is always a possibility of (adaptive) failure. Training should aim at strengthening capabilities that prepare individuals, teams and organizations to cope with challenges of variability in their environment and in their own functioning. Managerial mediation, intervention and intent are necessary to provide accountability, legitimacy and a defined space of manoeuvre. Managerial mediation of resilience is a capability that also benefit from, even require, training and a memory of successful practices.

2 THE TORC (TRAINING FOR OPERATIONAL RESILIENCE CAPABILITIES) PROJECT

2.1 Project background and structure

The TORC project is conducted by the SAF€RA TORC Consortium of experts and practitioners and include collaboration with industrial partners in all the three countries (Norway, The Netherlands and France), including offshore petroleum exploration and production, railway operation and maintenance and air traffic management. The specific *resilience in context* point of departure of TORC is thus appreciated both in terms of formal SAF€RA evaluation of the TORC project proposal, as well as the broad industry participation.

2.2 Rationale and objectives

Resilient properties of an organization emerge during operations. Most likely, they are destined to unfold under the imperative of compliance to rules or procedures inherent to management systems of organizations with high risk operations. This may imply that also resilience training must be conducted and orchestrated with a defined relation to prevalent safety (that is, compliance-oriented) training, aiming for a delicate balance between prescribed behaviour and adaptive abilities needed to cope with the unexpected. Such a training constellation comprises opposites that may appear as counter-intuitive, but practical experience suggests that "rudimentary" resilience in terms of tacit or silent adaptive practice is easier to appreciate when resilience as a principle (denoted "Safety II" by Hollnagel et al. 2013) is contrasted with the prevalence of compliance-based safety thinking (denoted "Safety I" by Hollnagel et al. 2013). This applies not at least from a managerial point of view, implying a shift of

[1] http://www.safera.industrialsafety-tp.org

attention to alternative modes of control in terms of articulating a space of manoeuvre to field staff, and thus also to increased reliance on and trust in their resilient capabilities. The appreciation of such "rudimentary" resilience, and the need to strengthen it, may be accentuated and made explicit by simulation or by reflection on action. This is seen as a very valuable point of departure when resilient properties needs to be further enhanced and developed, e.g. through training of key actors involved.

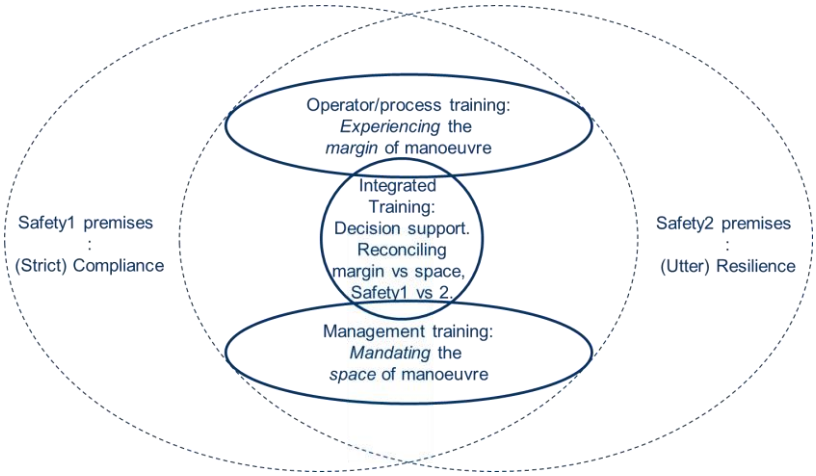


Figure 1. Three types of TORC training; distinctive but coherent. The precondition for using the TORC approach is that the "compliance base" (e.g., procedures) is well-defined, with a corresponding training activity in place. "Safety 1" corresponds to "Safety I", and "Safety 2" corresponds to "Safety II" in Hollnagel et al. (2013)

TORC discriminates between three types of training aimed at operational and managerial levels, and in their combination (Figure 1). The objectives are diverse, but mutually coherent in relation to the TORC rationale. In short, operational training invites the articulation of an *experienced and practiced margin* of manoeuvre, managerial training invites the articulation of a *mandated space* of manoeuvre that takes into account the possibility of adaptive failure, while integrated training aims for the harmonization and verification of the operational premises for these to meet in a manner in which resilient operations is aligned with the actual technical foundation, company mission and actual risk picture.

2.3 Aim and approach

TORC aims to develop an innovative training concept that enables organizations to appreciate, nurture and improve their inherent resilient and adaptive capacities, while being under the imperative of predominantly compliance-oriented safety regulations and standards. However, it is important to note that this is confined to the aspiration of enabling organizations to operate and *function more resiliently* under such circumstances, thus becoming able to cope with variability and surprise. Hence, the aim is *not* to transform them on the whole according to idealized forms of resilient systems, but to support them to develop resilient capabilities in a compliance-oriented context.

The approach is therefore to seek, identify and address actionable contexts in which organizations and their operations need to function resiliently in a compliance-oriented context. This is accomplished by interviewing and assessing cases of participating organizations. Rooted in evaluations of real and anticipated cases, the TORC aim can thus be pursued and operationalized. For that purpose, the TORC concept is founded on the presumption that the 'Compliance versus Resilience' (CvR) ensemble of relations (Grøtan 2015) encircles or resonates sufficiently with such a pragmatic context. TORC is developed and piloted in collaboration with industrial organizations that recognize the CvR relations as a relevant pragmatic context, and that strive for balancing compliance driven management with an adaptive complement and strategy. This attempt signifies not only an appreciation of the problem of predominant belief in the powers of prediction and rulemaking as a way of controlling operations. It also recognizes the limits of a more overarching and institutionalized imperative of "ruling by rule" that manifests in a whole range of situations and contexts for an industrial system, e.g., in design, commissioning, operation and maintenance.

It is important to note that by implication from the overall TORC approach, the concept of CvR relations carries no claim of explaining the functioning of a resilient system as a whole in relation to concepts of, e.g., advanced control loops, complex adaptive systems or other functional abstractions derived from systems science. Nevertheless, this does not preclude that TORC can take advantage of, e.g., Resilience Engineering as a rich source of concepts and

issues. The condition for doing this is however that the selected parts can be applied into the CvR context, and that they can be combined with recognized principles for training in general.

3 TORC FOUNDATIONS

3.1 Oppositions as (dialectical) drivers for progression

Bieder and Bourrier (2013) warn against "trapping safety into rules". The TORC point of departure is that resilience will unfold in a context of a "rational facade" urging for proof of control by relying on compliance to rules. This "facade" poses a shadow not only on the conditions *for functioning* resiliently, but also a potential shadow *hiding* the potential *merits* of resilient practice. Hence, resilience as an organizational property is positioned in the "contextual shadow of compliance" (Grøtan, 2013) where even its positive and needed contributions may remain unappreciated. This imperative of compliance is ubiquitous at every level, both inside and outside an organization seeking to develop its (rudimentary) resilience further.

Balancing the CvR relations is thus the primary underlying orientation for TORC, but this stance does however not purport to accommodate neither the full picture nor all nuances of safety in complex environments. It is first and foremost considered to be a useful position for the purpose establishing an actionable and pragmatic context for addressing and developing adaptive and resilient capacities under the imperative of compliance. It provides a scope of training in which a deliberate and dynamic reconciliation between adaptive coping practices and rule adherence/guidance is sought and practiced, including attention to dilemmas and preparation for the “unexpected”, beyond anticipation.

The second underlying theoretical position is the distinction/opposition between "Work as Imagined" (WAI) and "Work as Done" (WAD). Also this opposition rests on an underlying asymmetry with respect to status and impact within the organization; WAD is primarily associated with the realm of the operational, while WAI is primarily associated with the realms of design, engineering and management paradigms. A potential imbalance in this relation, e.g. that WAI by management and rule makers is predominantly and ingenuously compliance-oriented, while WAD is resilience-oriented but may lack managerial appreciation and attention to what is actually happening, is only one example of what may be detrimental for the attempt to benefit from the potential of resilience capabilities when adaptability in operations is needed to perform a task or mission.

The very foundation for the TORC approach is thus that resilient functioning can be gradually built by means of reconciling those two perspectives of opposing principles in a continuous and vigilant manner, however without insisting on permanent or persistent alignment. That is, the TORC approach is founded on the presumption that the appreciation of the inherent dialectics embedded in the two opposites may be a key driver for being able to keep pace with the evolving challenges posed by complexity and emergence in high-risk systems. On these premises, the TORC training will be designed to enable field staff and management to deploy resilient capabilities when needed.

3.2 Aspiration levels for expression of resilient functioning

Resilient behaviour can be associated with a repertoire of action. This is regarded as instrumental in order to train and develop for capabilities of resilient functioning in a gradual, stepwise and accumulative way. Available conceptualizations (e.g., Woods 2014/2015, Longstaff et al. 2013) are however regarded as too specific and comprehensive to be positioned as fully normative in the specific CvR/TORC context. However, they can be mobilized and offered as a theoretical inventory further down the road of a TORC training process, e.g. for the purpose of elaborating and deepening the pragmatic context as (TORC) training creates higher awareness and maturity, allowing companies and trainees to further elaborate the identification of routines, rules or knowledge based actions as the point of departure for resilient action. A TORC specific set of levels/grades will be used to signify a progression of resilient functioning (*in the context of compliance)*. These may assist in setting the levels of, e.g., decision support needed for allowing additional space of maneuver for adaptive alternatives needed to cope with unforeseen situations. The TORC levels are as follows:

R1. *Defend* normalcy (preferred mode of operation)

R2. *Build* robustness to anticipated disturbance

R3. *Stretch* and rebound in an (isolated) surprising situation/episode

R4. *Sustain* resilient functioning over time.

Hence, aspirations to fully exploit the resilience potential of an organization range from R1 to R4. The scale thus commence (R1) from a comparatively simple notion of a well-defined and confined response based on a specific

protocol. At the other end, resilient functioning may take the form of a more boundless intra- or inter-organizational mobilization; as an ultimately emergent response to a novel challenge or demand.

3.3 Bringing the resilient "emerging fresh produce" under managerial accountability

Resilient functioning (and even "resilience") may be seen as an "emerging fresh produce" which must be maintained, refreshed, reinforced and renewed. Training and rehearsal is an essential part of this, including feedback of experience, e.g. by after action review of resilient operations. This makes tacit behavior explicit and identifies relevant findings that need to be memorized and transferred to the organization's management, in order to improve or expand resilient capabilities. TORC aims to enable and facilitate a systematic effort of training in order to bring forward, recognize, label, nurture, develop and bring resilience under managerial influence, control and accountability, in a stepwise and measuredly balanced way. The intended effect is to facilitate a process by which resilient functioning as an organizational property, despite its inevitable "bottom-up" character, is appreciated, explicated and brought out of the "contextual shadow" of compliance, and also brought under a measured degree of managerial intent, supervision and accountability.

3.4 Extended focus; CvR reconcilations

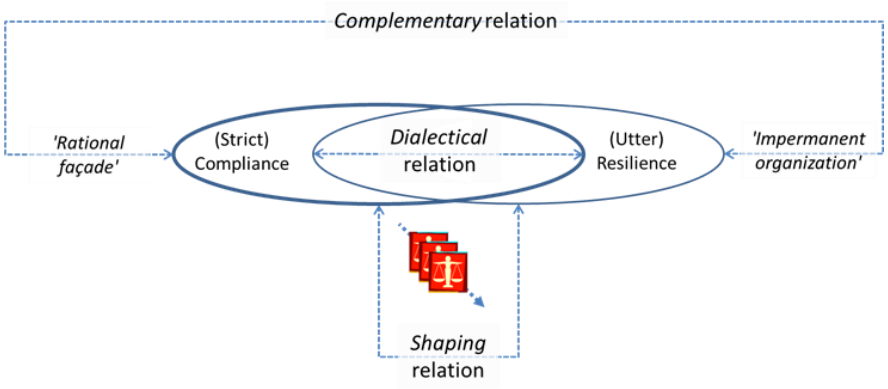


Figure 2. The CvR complementary, dialectical and shaping relations (Grøtan 2015)

With resilience positioned also in a *shaping* relation with compliance (Figure 2), the rationale for TORC is not confined to resilient functioning in the strictest sense. TORC also aims at being a vehicle for a productive co-creation of functional and effective rules (that is, compliance) and trustworthy and reliable adaptive capacities (that is, resilience), in conjunction. CvR reconciliation thus also implies an act of mutually measured CvR calibrations, aiming for increased resilience, complementing optimization of rule effectiveness and efficiency. While the "rational facade" tend to rest on a machine metaphor (Morgan, 2006) for the stable and enduring organization, the resilient contribution rests on a more organic and adaptive organizational metaphoric, ultimately pointing towards "organized impermanence" as described by Weick (2009).

3.5 The presumed non-linearity of resilient functioning

The TORC aspiration scale (R1-R4) is as non-linear as the more precise definitions it is inspired by. The very character of the challenge encountered and resolved will change along the progression. Hence, also the characteristic of the stepwise resilience capability achieved by an organization may have to be revised in a longer perspective. Some key implications can be envisaged through the Law of Stretched Systems (Woods, 2014), by seeing consecutive episodes of resilient practices and an increased set of capabilities and real adaptations as a manifestation not solely of increased control, but also of shifting boundaries of complexity, and potential new origins of future surprises.

TORC training progression will nevertheless imply a premise of a dynamically changing orientation underlying the resilient functioning, commencing with explication of the adaptive practices that are associated (e.g.) with rudimentary resilience, proceeding with the successive needs for interpretation and then reduction of equivocality by means of sensemaking (Brown et al. 2015), and ultimately ending up in a situation of stability-focused intervention in terms of sheer improvisation; to act, sense and then respond further.

3.6 Training and learning

The TORC approach discriminates between three types of learning and reflection.

- Rule-centric learning: translating adaptive experiences into rules, procedures or protocols that enhance the chances of coping with similar events at a future occasion
- Adaptation-centric learning: preserving key features of adaptive experiences in ways that enhance the chances of success at a future surprise.
- Reconciliation-centric learning: improving the understanding of the CvR balance, and learning to identify reconciliations that provide a good climate for responsible trade-offs implying, e.g., a decision support framework and available resources to be mandated to respond in a resilient way.

Narratives are seen as important as containers of experiences. They may be distilled into rule-centric or adaptation-centric aspects, but they are not at least potentially useful for representing the combined and reconciled, including the managerial influence and facilitation. Facilitating reflection on action and preservation of results in repositories of experience and evaluations of effective resilient operations, is therefore an important part of intra- as well as inter-organizational utilization of the TORC approach.

3.7 Key issues for a TORC-based training program

Given that the "strict compliance" is recognized as a management paradigm denying the pragmatic context of everyday operations, operational experience must be brought to the fore to understand, legitimate and appreciate rudimentary resilience, which subsequently may be characterized/assessed along the R1-R4 scale. From then, improved resilient functioning (R1-R4) can be gradually introduced in the context of procedural training. During training, changing orientations (explication, interpretation, sensemaking and communication) will be encountered, but also a changing imperative ranging between, e.g., (a) the rule-centric reconciliation: how does resilience support compliance? and (b) the adaptation- centric reconciliation: how do procedures provide a resource for resilience?

This implies that TORC aims both at preparing for resilient dynamics in practice but also at reflection on action, explicating experience of coping with challenges by adaptive behavior. The knowledge elicited gives input to the resilience memory or repository being used for further developing the organizations performance, e.g. for training, changes in rule making and opening up spaces of maneuver by changing strategies to benefit from improved resilience capabilities.

4 STRUCTURING A TORC TRAINING PROGRAM

4.1 Underlying structure aiming for reuse, sharing and mutual development

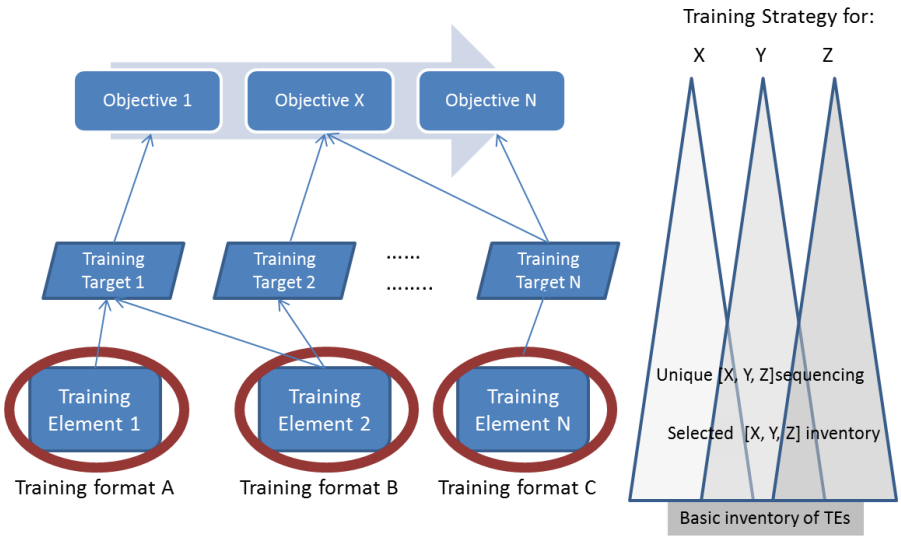


Figure 3. TORC training structure. Training Objectives, Targets, Elements, Formats and Strategies". Strategies X, Y, Z also signifies potential reuse across different industries

The TORC project will structure the activities and document the results according to the structure in Figure 3. The (generic) Training Targets (TT) are operationalizations of the TORC rationale and objectives for practical training purposes. A Training Element (TE) is a unit of distinct training aiming at one or more TTs. A Training Format (TF) is a specific way of conducting a TE (e.g. by off-line training, on the job, gaming etc). Training Elements chosen may be aimed at sensemaking, organizing decision support, team communication, deployment of resources (etc).

Training targets of TORC are aimed at training both sharp end (field staff) and blunt end (management), separately and together.

Specific Training Elements (TE) and Training Formats (TF) constitute generic entities for implementing specific TTs in a manner that can be re-used across companies. A Training Strategy (TS) is a compilation of TEs (and TFs) that is arranged and conducted in a training design for the purpose of a specific organization, its needs and preconditions.

Hence, connected Training Strategies (TS) can be built from common objectives, shared TTs and generic TEs/TFs, based on a basic/minimum TE inventory. The TORC pilots may thus be seen also as TS pilots, building on a shared repository of TT, TE and TF being aimed at strengthening particular capabilities sought by participating companies. A guideline will be developed on how to make a subset of these objectives, TT and TE/TF as a part of the "priming" for a TORC training program design. A shared repository of generic TEs will also be proposed. However, the TORC structure is designed for the purpose of being used also after the TORC project and will be published, inter alia, by FonCSI.

The TORC project will also seek to tailor this generic structure to more specific contexts in terms of (1) normal operation, (2) emergency training and (3) management of unexpected situations.

5 RELEVANCE FOR MANAGING RESILIENCE

The relevance for managing resilience is constituted by the description of a distinct and grounded managerial position related to the aspiration of "control" over resilience in the pragmatic context of the "rational facade", both by operations at the sharp end and management at the blunt end. Although the CvR and TORC approach clearly does not claim to be "true" for the purpose of Resilience Engineering in general, the offering of a CvR-based management training program on TORC capabilities, in conjunction with operational training, is considered an important contribution for learning to be adaptable and proactive in an unpredictable world.

6 CONCLUSION

TORC addresses managerial practices and training in conjunction with operational training, emphasizing that this should be conducted in an organizationally coherent manner and being adaptable to local context. The TORC training approach to resilient capabilities is thus expected to be relevant and applicable for a wide range of organizations as well as researchers that are occupied with reinforcing, creating and sustaining resilient functioning. The training pilots will take place in concurrent company developments, and will seek to explicate a resilient experience repository, supported by experience feedback and evaluations for further progress in resilience capabilities. The TORC project transfers practical experience and knowledge provided by a cooperation of research institutes with participating companies in the domains of off/on shore oil drilling, a high speed infrastructure provider and a railway contractor.

The TORC approach is meant to be supportive of Resilience Engineering[2] in a "compliance context" (Grøtan 2015), with a deepened association with the social sciences. In the latter sense, TORC resonates not only with Giddens' (1987) "double hermeneutic" position from the more distant realm of the social sciences, but also - more importantly - with renowned scholars in the field of safety science, e.g. Weick (2009) and Perin (2006).

Acknowledgements

The work reported in this paper is based on a grant from the *Norwegian Research Council* and the *Fondation pour une Culture de Sécurité Industrielle* (FonCSI) through SAF€RA, and contributions of TNO, SINTEF, Dédale and cooperating companies; Eni Norge (NO), NAM, Strukton Rail and Infraspeed (NL).

REFERENCES

Bieder, C., Bourrier, M. (2013). Trapping Safety into Rules. How Desirable or Avoidable is Proceduralization? Ashgate

Brown, A.D., Colville, I., Pye, A. (2015). Making Sense of Sensemaking in Organization Studies. Organization Studies Vol. 36(2) pp 265-277 (http://oss.sagepub.com/cgi/collection/making_sense_of_sensemaking)

Giddens, A. (1987). Social Theory and Modern Sociology. Cambridge, Polity Press

[2] 'the scientific discipline that focuses on developing the principles and practices that are necessary to enable systems to function in a resilient manner' (Hollnagel, 2014, p.183)

Grøtan, T.O. (2013). Hunting high and low for resilience: Sensitization from the contextual shadows of compliance. In Steenbergen et al. (Eds): Safety, Reliability and Risk Analysis: Beyond the Horizon. Taylor & Francis Group, London

Grøtan, T.O. (2015). Organizing, thinking and acting resiliently under the imperative of compliance. On the potential impact of resilience thinking on safety management and risk consideration. PhD thesis (2015:86) at the Norwegian University of Science and Technology. Trondheim. Norway, April 2015.

Hollnagel, E., Leonhardt, J., Licu, T., Shorrock, S. (2013). From Safety-I to Safety-II. A White Paper. EUROCONTROL (European Organisation for the Safety of Air Navigation).

Hollnagel, E. (2014). Safety-I and Safety-II. The Past and Future of Safety Management. Ashgate

Longstaff, P.H., Koslowski, T.G. and Geoghegan, W. (2013). Translating Resilience: A Framework to Enhance Communication and Implementation. Proceedings of 5th Resilience Engineering Symposium,

Morgan, G. (2006). Images of organizations. Sage Publications

Perin, C. (2006). Shouldering Risks: The Culture of Control in the Nuclear Power Industry. Princeton University Press,

Weick, K.E. (2009). Making sense of the organization: Volume Two: The Impermanent Organization. John Wiley and Sons

Woods, D. (2014) Outmaneuvering Complexity. Releasing the Adaptive Power of Human Systems. Presentation at Workshop for TORC-Project 27 October 2014 Paris, France

Woods, D. (2015). Four Concepts for resilience and the Implications for the Future of Resilience Engineering. Reliability Engineering and System Safety, http://dx.doi.org/10.1016/j.ress.2015.03.018

EXPERIENCES IN FUKUSHIMA DAI-ICHI NUCLEAR POWER PLANT IN LIGHT OF RESILIENCE ENGINEERING

Atsufumi Yoshizawa [1], Kyoko Oba[2] and Masaharu Kitamura[3]
[1] Nuclear Fuel Transport Company
1-1-3, Shiba Daimon, Minato-ku, Tokyo, 105-0012 Japan
E-ail atsufumi_yoshizawa@nft.co.jp
[2] Japan Atomic Energy Agency
2-2-2, Uchisaiwai-cho, Chiyoda-ku, Tokyo, 100-5877, Japan
E-mail oba.kyoko@jaea.go.jp
[3]Research Institute for Technology Management Strategy (TeMS)
6-6-40-403 Aramaki-Aza-Aoba, Aoba-ku, Sendai, 980-8579 Japan
E-mail kitamura@temst.jp

Abstract

The conventional concept of safety had the objective to eliminate risk. However, the Fukushima Daiichi Nuclear Power Plant Accident exemplified that there is a region of safety that cannot be covered by such an approach. As is evident from the first author's experience on site during the Fukushima Accident, systems need to be resilient in order to secure safety even amidst large disturbances. Also, people in the field showed the ability to make an effort to achieve success (recovery) even when plagued by problems or adversity (resilience). This paper introduces a model for explaining the difference between conventional and new safety concepts. As this model requires the analysis of success cases, this paper focuses on incidents within the Fukushima Accident and analyzes two incidents that can be considered successes based on Resilience Engineering methodology. Based on this analysis, we attempt to structuralize the relationship between the four core capabilities of Resilience Engineering (Learning, Responding, Monitoring, and Anticipating) and complementary traits in order to utilize Resilience Engineering in real-world situations.

1 INTRODUCTION

The objective of the conventional concept of safety is freedom from unacceptable risk. In other words, the premise is that safety can be achieved if risk factors, which are foreseeable, are removed from the system. However, the accident at the Fukushima Daiichi Nuclear Power Plant (Fukushima Accident) , which was caused by an M 9.0 earthquake triggered by an unprecedented motion of tectonic plates that caused a 15 m tsunami (estimated height at Fukushima Daiichi NPP), clearly demonstrated there are exigent circumstances for which this conventional approach does not apply (TEPCO, 2012). This paper proposes the necessity for a new safety concept that transcends this conventional concept and reexamines the positioning of humans within safety concepts.

The first author was the Plant Manager of Fukushima Daiichi NPP Units-5/6 at the time of the Great East Japan Earthquake and was put in a position where he had to cope with the accident in a way that would ensure the safety of site personnel while providing a response to the site emergency. When the power plant lost power, lighting, communications, instrumentation and monitoring functions became severely impaired. These conditions combined with exploding buildings and spiking radiation levels plunged the power station into a situation that far exceeded plant design basis. Just maintaining the status quo required multiple tasks, including supplying fuel to fire engines and power trucks used to cool the reactors, which had to be carried out under extremely challenging conditions with limited resources. In addition, as various manuals with which plant operators had boasted compliance were being rendered useless, the author was put under enormous pressure to respond quickly and flexibly to the situation based on uncertain information.

It is clear that under such severe accident conditions the situation would have most certainly escalated to catastrophic proportions had it not been for the actions taken at the site. None of the critical actions taken at the site, including injecting water into the reactors, were done automatically—they were the sole response of the people at the plant. However, conventional safety assessment methodology has always considered humans as "elements which threaten system safety by causing human error," so systems were designed to remove this fluctuating element from the system as much as possible. As the people on-site desperately coped with the accident I witnessed behavior that was completely opposite from what was defined by the conventional safety

concept—they actually possessed the ability (resilience) to think and flexibly respond in order to restore systems in a changing environment (Hollnagel and Woods, 2006).

The Fukushima Accident showed us that a resilient system is a vital for securing safety, i.e., the system needs to be able to avoid catastrophic failure even amidst large disturbances and that this will eventually be achieved through human actions. This is in perfect concert with the concept of Resilience Engineering (Hollnagel et. al., 2006, 2010). It also demonstrates the validity of Resilience Engineering methodology that puts forth the response by people as one of its core capabilities.

This paper attempts to pursue higher standards of safety by focusing on the actions of the people who responded to the accident on site and evaluating specific events during the accident based on a new "people-focused" safety concept while referring to Resilience Engineering, which has been recently proposed and is in the process of development. It should be noted that the examples described in this paper will be categorized as Unexplained Events as per Westrum's Typology of Resilience (Westrum, 2006) and, accordingly, this paper examines the ideal state of resilience under such conditions.

2 NECESSITY FOR A NEW SAFETY CONCEPT (SAFETY-II) AND THE RESILIENCE ENGINEERING APPROACH

In this section summaries of relevant preceding studies that evaluate the events that occurred on site during the Fukushima Accident will be provided along with an explanatory model used to deepen understanding of the differences between conventional thinking.

2.1 Concepts of Safety-I and Safety-II

In the past, safety was constructed on the basis of minimizing risk, i.e., safety will be achieved by predicting accident events, identifying the risks leading to such events, and removing such risks therby preventing accidents from happening. However, flexible responding in different ways during an emergency is only possible by humans and the organizations that they comprise, and as such, a new goal needs to be set that will nurture capabilities that can be applied in an agile manner.

Recently, Hollnagel defined the existing safety concept as Safety-I and the new safety concept as "Safety-II" (Hollnagel, 2014). The latter is defined further as "safety as the ability to succeed under varying conditions" and the target to achieve is described as "a condition where as much as possible goes right"(Hollnagel, 2014, pp134). The humans are considered as "a resource necessary for system flexibility and resilience" (Hollnagel, 2014, pp147). This new notion of safety differs from Safety-I that emphasizes the minimization of risk in that it focuses rather on identifying those actions that increase the chance of success and exemplifies the capabilities displayed by the people and organizations at the site of Fukushima Accident.

2.2 Importance of Learning from Successes Hidden within Larger Events

A typical definition of Safety-I is"Freedom from risk which is not tolerable (ISO/IEC Guide 51)", according to which safety is constructed with a focus on risk and failure. Analyzing failures and preventing recurrence by removing the cause is a typical application of Safety-I, which is based on the "hypothesis of different causes" that considers failure and success to be the resultants of different factors (Hollnagel, 2014, pp.52).

However, in large-scale socio-technical systems such as nuclear power plants, things are more complicated. Figure 1 shows a concept diagram during normal times and emergencies. The iceberg depicts a collection of actions and examples. In complex systems, it is appropriate to express incidents as a collection of many actions and examples. The water surface depicts the competence of the organizations and people. As shown in Figure 1, during normal times aseries of actions are conducted within the capacity of people and organization in order for the system to function, and fluctuation can be absorbed.

This figure shows that two approaches are necessary to ensure safety during a single event. The first is to ensure prior preparation so that failure, as depicted in Figure 1 by the portion of the icebergiceberg above the water's surface, does not occur again. The second is to equip [the system] with capabilities that will enable the success of various tasks to be processed smoothly and effectively , as depicted by the portion of the icebergiceberg below the water's surface, and to minimize the portion of the iceberg above the surface. Actions taken during the Fukushima Accident that were below the surface were, for example, cooling the reactors by injecting seawater using fire engines and providing power to instruments in the control room using car batteries(TEPCO, 2012, Capter8). Detailed examples will be described in 3.1 and 3.2.

As described in the second approach to ensuring safety, the height of the water surface in Figure 1 (span of capability) can change significantly according to the situation and the interaction between the organizations and teams that respond to the accident. In other words, people are doing their best as every moment passes by and making decisions based on bounded rationality with the information available at the time. The distinction between failure and success can only be made after the fact and are not necessarily the result of separate factors (parity of success and failure.) Therefore, failure events can be viewed as having failed by chance under a certain situation. As the concept of Safety-II shows, it is not appropriate to think that causes for failure and success are different by applying the hypothesis of different causes to the upper and lower parts of the iceberg.

Based on the experience of the Fukushima Accident, the first author confirmed the necessity for a paradigm shift from the conventional Safety-I that pursues safety by focusing on failures to Safety-II that aims to elicit efforts to maximize the chance of success.

Note thatfailures within the portion of the actions and events that run the system and usually go on unnoticed under water but that "emerge" above the surface during a disaster, provide an opportunity to notice issues. It is important to have the capability to learn from these opportunities by discovering resilient events that hide behind the shadow of failures.

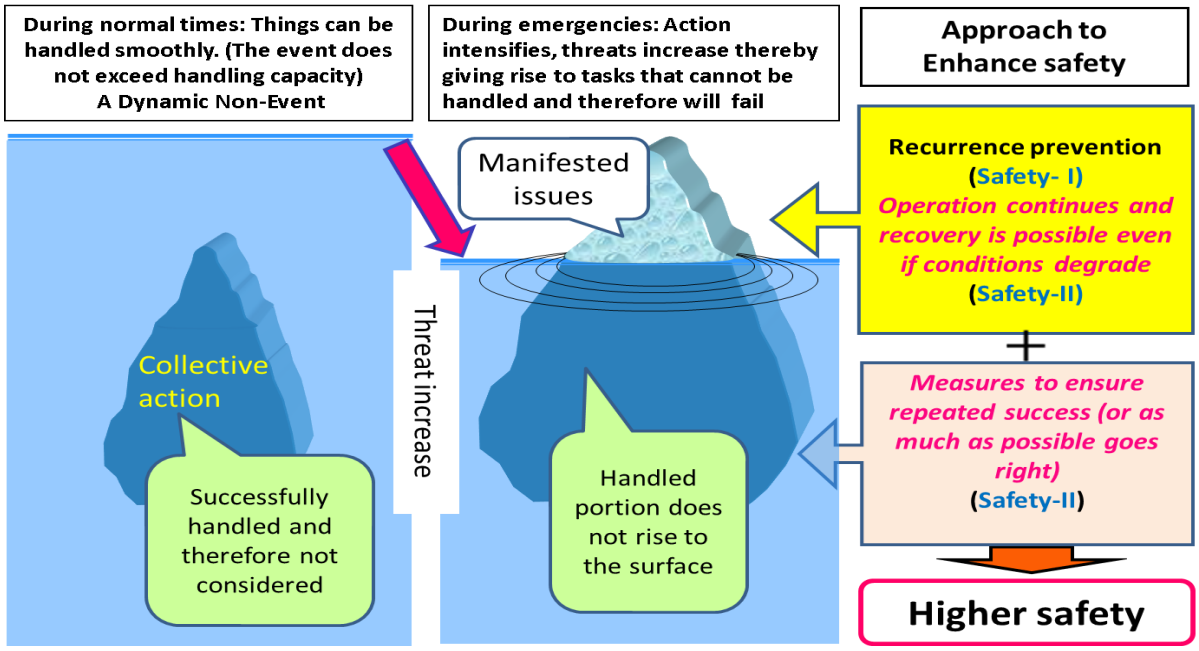


Figure 1. Comparison model of approach to enhance safety between Safety-I and Safety-II

Disasters visualize social systems for what they really are, and provide opportunity discovering resilient events

2.3 Resilience Engineering and its Components

Resilience Engineering has recently been widely recognized as a methodology to pursue safety based on Safety-II. The purpose of Resilience Engineering boils down to how to bring about resilience (elasticity and recoverability) to systems.

It is well known that Resilience Engineering defines the following four elements as core capabilities (Hollnagel, 2009):

- Learning,
- Responding,
- Monitoring,
- Anticipating.

These four capabilities are not independent of each other but rather interact. The capabilities of Responding and Anticipating can be improved through study and practice. If anticipation is successful, response capability improves. Conversely, extremely high response capability can in some cases make up for a lack of anticipation. However, even if there is a difference in the degree of aptitude between them all four capabilities are necessary for a system to have resiliency.

Further complementary requirements need to be met in order for these four capabilities to effectively function. . Hollnagel and Woods pointed out that deficiencies in time, knowledge, competence, and resource will force a system to lose control and noted that resolving such deficiencies is a condition for resiliency (Hollnagel and Woods、2006). The authors summarized these conditions as complementary prerequisites as follows:

As system is forced to operate in a passive mode when time runs out, so it is important to increase system anticipation and take proactive measures to secure time. Knowledge and competence are prerequisites for making decisions on how to respond, but to make such decisions, learning from successes, as mentioned in 2.2, is also important. Knowledge and competence means knowing what to do and how to do it, but the appropriate allocation of resources is critical in order to take necessary action. It is pointed out that the capability to notice subtle changes is necessary in order to initiate the functions of responding and monitoring(Lay,2010). Given the above discussion, this study will focus on “proactive actions”, learning from “successes”, preparation and the appropriate allocation of “resources”, and the capability to take “notice” as four complementary prerequisites. Although “knowledge and skill (competence)” are equally important, it is not a prerequisite specific to Resilience Engineering but rather to operational safety in general. Therefore, these are treated as more basic prerequisites compared to the four complementary prerequisites. Note, however, that proactive measures may well end up being unnecessary. Organizations that stress resilience need to have a business strategy that accepts sacrifice decisions (Woods, 2006).

3 THE CASE OF FUKUSHIMA DAIICHI NPP

In this section, the , relationship between the four core capabilities of Resilience Engineering described in Chapter 2 and the four complementary prerequisites will be examined based on actual case events at the Fukushima Daiichi NPP. As mentioned before, disasters enable us to visualize systems and provide opportunities to notice various elements. Numerous reports were made after the accident but the vast majority of them focus on failures with very few discussing successes. This section will shed light on successes that have not been studied in any report and will be evaluated based on first-hand experience on site by the first author.

3.1 Case 1: Emergency Evacuation of a Heavy Oil Tanker (TEPCO, 2012, Appendix 2, pp.7)

When the earthquake occurred a tanker was moored in the power plant port where heavy oil was being transferred from it to a tank via a pipeline. When the earthquake struck, the onshore manager (experienced with operating ships) and the captain of the ship anticipated the arrival of the tsunami based on their experience (learning effect.) The captain immediately made the decision to evacuate the tanker from the port and move it

out to sea. At the time, the captain also made the decision to prioritize emergency departure from the shore and to cut and abandon the pipeline and oil fence, based on the time required to take such actions. The tools (resource) required to cut the oil fence were on-hand. As a result of this quick decision-making and maneuvering of the ship amidst sea currents that were already being affected by the approaching tsunami, collisions with other ships and floating debris (coping and monitoring) were avoided and the tanker was moved out of the port just in time to prevent damage from the tsunami.

If the evacuation had been delayed and the tanker had been stranded onshore, not only would it have become an obstacle for the emergency response, but it could have also caught on fire and exacerbated the situation. As such, this is an important case that contributed to preventing further deterioration of the conditions on site.

3.2 Case 2: Explosion Prevention at Fukushima Daiichi NPP Units 5 and 6 Reactor Buildings (TEPCO, 2012, Appendix 2, pp.151)

Among the six units at Fukushima Daiichi NPP, Units 1 to 4 incurred severe damage. However, Units 5 and 6 were also far from safety. Fortunately, an air-cooled emergency diesel generator installed in Unit 6 survived the tsunami and was able to operate continuously. This enabled the supply of power, albeit insufficient, to Unit 5 that had lost all AC power. Thanks to this generator just enough power was provided to keep monitoring instruments in the main control room working and restore the residual heat removal system. In hindsight, enabling water levels in the reactors and spent fuel pools to be maintained prevented the generation of hydrogen gas. However, when the building for Unit 4, which was undergoing periodic inspection just like Units 5 and 6, exploded, the cause of the explosion was unknown and it was not unreasonable to assume that Units 5 and 6 might suffer the same fate. Also since power was supplied by an emergency diesel generator that was vulnerable to singular failure the possibility that aftershocks could disable water injection and heat removal functions was foreseeable. Hence, in the early morning of day seven, holes were drilled in the concrete roofs of the Unit 5 and 6 reactor buildings using boring machines. Although worker safety was of the utmost concern, the decision to carry out the task was made from a more macro-safety point of view. This eliminated the risk and concern of hydrogen explosion thereby enabling work to bring the units to cold shutdown on day nine to continue. This measure was flexible, proactive and significantly different from normal safety procedures.

In the process of carrying out this task, large construction companies turned down TEPCO's request for personnel support and only provided other resources, such as equipment. Just when TEPCO personnel started to take actions on their own they ran into the office manager of a local building contractor, who volunteered to help. Thanks to inter-organizational team work and determination another crisis was avoided.

3.3 Voices from the Field

In order to explain responding to avoid extreme conditions, there are cases in which the four complementary prerequisites described in Section 2 fall short. Case 2 is a clear example. For the office manager of a building contractor, there was no reason to volunteer to help with such a dangerous task especially since he was in the process of evacuating. Later, he reflected on his decision to help saying that he felt that if he did not volunteer to go along he wouldn't be worthy enough to work at the power plant again for the rest of his life. It is apparent that this decision was made because of the feeling of unity between TEPCO employees and contractors that had been cultivated through daily operations.

Below we examine these incidents using excerpts from interviews with another people involved.

- "For operators to leave the control room, it means giving up control of the reactor. That means abandoning the evacuated local residents who have put their faith in us as well as our own families. That is why we cannot just leave. " –Quote from shift manager addressing his subordinates and then bowing deeply. (Takahashi, 2015)

- I will do anything. I am prepared to throw myself into the jaws of the power station. If there's anything that needs to be done, just tell me. I want to show you that operators have guts if it's the last thing I do. (Veteran TEPCO personnel with much experience in operation)(TEPCO, 2012, pp184)

- With a sense of mission as a plant contractor and the knowledge of how hard Masao Yoshida was fighting to save the plant, I simply could not abandon him. (Chief of local office of a plant contractor) (Takahashi, 2015)

What can be seen from these words is that it was the optimistic attitude of the workers involved in this situation

that enabled various tasks to be carried forward. This "Attitude" was cultivated by various factors including the sense of mission and solidarity of field workers to restore systems anyway they could amidst accident condition, and the sense of attachment to their local community in Fukushima. From among the four core capabilities of Resilience Engineering emphasis should be placed on the importance of Attitude as it is a critical factor for facilitating an effective response, as (Komatsubara, 2008)(Oba, et. al., 2014)(Yoshizawa, et. al.,2014).

3 DISCUSSIONS AND CONCLUSIONS

Since the wake of the Fukushima Accident, numerous discussions have been ongoing with regard to the concept of safety for large-scale socio-technical system. The conventional concepts of safety had the objective of freedom from unacceptable risk and considered system risk factors could be foreseeable with the assumption that safety could be achieved by eliminated them. However, the Fukushima Accident illustrated that there is a region of safety that cannot be covered by such an approach and that there is a need for a new safety concept that transcends this conventional concept. As is evident from the experience on site during the Fukushima Accident, systems need to be resilient in order to secure safety and these system need to be able to avoid catastrophic failure even amidst large disturbances. This is in perfect concert with the concept of Resilience Engineering, i.e. "safety is the ability to succeed under varying conditions (Hollnagel 2014)".

Historically, humans had been treated as "elements which threaten system safety by causing human error." However, workers in the field during the Fukushima Accident desperately fought the accident and possessed the ability (resilience) to flexibly think and take action to restore systems in a changing environment. It was concluded that Resilience Engineering as a methodology for achieving Safety-II that identifies four core capabilities, and complementary prerequisites that nurture such capabilities, for humans and organizations, is an effective method for leveraging the lessons learned from first-hand experience during the Fukushima Accident.

This paper introduced a model to explain the difference between Safety-I and Safety-II concepts. A model showed the necessity to focus on successes and also showed that failures and disasters have enabled systems to be visualized and have provided opportunities to recognized hidden events that are resilient.

The paper also focused on smaller events within the Fukushima Accident and analyzed two successes based on Resilience Engineering methodology. The importance of Attitude as a trait that complements the four core capabilities was pointed out. Furthermore, an attempt was made to identify complementary prerequisites in preparation for practical application.

Acknowledgements

We would like to express our heartfelt apologies to the many people who still are leading lives as evacuees due to the Fukushima accident as well as for all the inconvenience and anxiety the accident has caused the local community and Japanese society as a whole. In addition, we would like to express our appreciation for the support of so many people who devoted themselves to responding to the accident under such severe conditions, and our condolences to the families of the two colleagues who made the ultimate sacrifice in the line of duty and Site Superintendent Masao Yoshida, who spearheaded the initial response.

REFERENCES

Hollnagel, E.(2009). *The Four Cornerstones of Resilience Engineering.* In Nemeth C.P., Hollnagel E.and Dekker, S. (eds.) Preparation and restoration, Resilience Engineering Perspectives, Vol.2, Ashgate.

Hollnagel, E.(2010). Prologue: *The scope of Resilience Engineering,* In Hollnagel, E., Pariès, J., Woods, D. and Wreathall, J. (eds.). *Resilience Engineering in Practice : A Guidebook*. Ashgate.

Hollnagel, E. (2014). *Safety-Ⅰ and Safety-Ⅱ, The Past and Future of Safety Management.* Ashgate. (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.

The International Organization for Standardization and the International Electrotechnical Commission (2014). Safety aspects- Guidelines for their inclusion in standards, Guide 51.

Komatsubara, A.(2008). When Resilience does not Work. In Hollnagel, E., Nemeth, C.P. and Dekker, S.(eds.) Remaining Sensitive to the Possibility of Failure, *Resilience Engineering Perspectives, Vol.1, ,* Ashgate.

Lay, E.(2010). Practices for Noticing and Dealing with the Critical. A Case Study from Maintenance of Power Plants. In Hollnagel, E., Pariès,J., Woods, D. and Wreathall, J. (2010). *Resilience Engineering in Practice : A Guidebook,* Ashgate.

Oba, K., Yoshizawa, A. and Kitamura, M. (2014). Enhancement of Organizational Resilience in Light of the Fukushima Daiichi Nuclear Power Plant Accident (II) – Promoting of Attitude Building Measures -, *The Japan Society of Mechanical Engineers, Proceedings of the 2014 Annual Conference, G2010103.* (In Japanese).

Takahashi, H., Kyodo News Nuclear Accident Coverage Team Editor (2015). *Remembrances of the Loss of All Power Supply.* Shodensha (March 6, 2013). (In Japanese)

Tokyo Electric Power Company, Inc. (2012). *Fukushima Nuclear Accident Investigation Report.*

Woods, D.D.(2006). Essential Characteristics of Resilience. In Hollnagel, E., Woods, D. and Leveson, N(eds.). *Resilience Engineering : Concepts and Precepts,* Ashgate.

Westrum, R. (2006), Typology of Resilience. In Hollnagel, E., Woods, D. and Leveson, N.(2006). *Resilience Engineering : Concepts and Precepts,* Ashgate.

Yoshizawa, A., Furuhama, Y., Mutou, K., OBA, K., and Kitamura, M. (2014). Enhancement of Organizational Resilience in Light of the Fukushima Daiichi Nuclear Power Plant Accident (I) – Analysis of Responding Structure -, *The Japan Society of Mechanical Engineers, Proceedings of the 2014 Annual Conference, G2010102.* (In Japanese).

EXPERIENCES FROM AVIATION: OPERATIONS AND TACTICAL COORDINATION IN THE COCKPIT

MANAGING THE RESILIENCE OF PILOTS IN THE COCKPIT

Christian Kunz and Toni Waefler

Institute Humans in Complex Systems, School of Applied Psychology, University of Applied Sciences and Arts Northwestern Switzerland, Riggenbachstrasse 16, 4600 Olten, Switzerland; www.fhnw.ch/miks

christian.kunz@fhnw.ch (+41 79 784 80 14)

Abstract

In aviation, several accidents, incidents and near-misses happened in 2014. These made obvious that the high safety standards and successful operation in the past cannot guarantee future successful operation. Therefore, assuring safety is an ongoing process, especially in high risk industries like aviation.

The aim of this study was to operationalize Hollnagel's (2011) four essential capabilities of resilience (subsequently referred to as "fecor", i.e. the abilities to monitor, to anticipate, to respond, and to learn) with regard to pilots in the cockpit of Swiss International Air Lines. Based on this operationalization an instrument was developed, allowing for measuring the pilots' resilience and hence for a proactive trend monitoring. In accordance with core assumptions of Resilience Engineering and Safety-II this study focused on "things that go right" (Hollnagel, 2012, 2014), on "normal functioning" (Hollnagel et al., 2013, 2014), and on "work as done" (Dekker, 2006).

The study was carried out in two phases. The aim of the first phase was to operationalize the fecor and thus to understand how pilots create and sustain resilience, i.e. how they adapt to potential and actual changes during a flight to sustain normal functioning. Phase one had the following three steps:

In step one a systematic qualitative content analysis of literature was conducted. The results show, that the fecor can be differentiated per ability with several main- and subcategories. In the core there is the main category "activity" consisting of the subcategories intended "outcome", resilience specific "behavior", and "method". Prerequisites, which are critical for executing ability-specific activities, represent another main category. To give an example: The subcategory "behavior" of the ability to monitor contains specific monitoring behavior like "updating of beliefs" or "recalibrating risk models", the subcategory "method" contains behavior-supporting methods like "cross-checking" or "information gathering", and the subcategory "outcome" contains e.g. "recognize changed situation" or "noticing critical disruptions".

The aim of step two was to concretize these theory-based categories with reference to the pilots' task. To do so, five semi-structured expert interviews with pilots were conducted and analyzed with qualitative content analyses. The interviews aimed at identifying dimensions with variability, i.e. dimensions that could change in a system-relevant manner and thus require adaptation from the pilots. Subsequently, the fecor-specific adaptation activities as well as the respective prerequisites were identified. The results show that there are several dimensions with variability, e.g. "technical aspects", "human aspects" or "weather". Furthermore, first leading indicators could be defined which refer to the pilots' adaptive behavior to potential or actual changes in order to sustain normal functioning. In the study it was decided to focus the subsequent steps on resilience related to potential or actual changes in the dimension "weather". This focus has been chosen because of the fact that weather is to a certain amount unpredictable for a system. Furthermore, the technical systems on board often do not automatically provide information about possible weather changes, especially not regarding the more distant future, which may become system-relevant. Therefore, the pilots' anticipation and monitoring concerning weather are crucial.

In step three a semi-structured group interview with five pilots was conducted in order to deepen and to verify the previous results. Final results of this step are four fecor-specific models of leading indicators. These models describe the pilots' resilient activities (behavior, methods and outcomes) as well as the related prerequisites required to successfully cope with variability in the dimension "weather". For the ability to monitor, behavior-specific leading indicators are e.g. "communicative information exchange" or "assessment of recognized changes". A Related method-specific leading indicator is e.g. "active acquisition of information". The subcategory "outcome" then contains e.g. the indicator "recognition of system relevant changes in the weather". Indicators for prerequisites are e.g. "knowledge about current main focus" and "situation awareness".The aim of phase two was to develop an instrument for measuring the fecor. For that purpose a questionnaire was developed referring to the behavior of pilots in the cockpit. An item analysis as well as a

reliability analysis with regard to the internal consistency (Cronbach's Alpha) were conducted on the basis of a online survey completed by 134 pilots. The results showed that the fecor can be measured with 93 psychometrically suitable items in 17 reliable scales (Cronbach's Alpha between α=.66 and α=.89). These reliable scales thus enable a proactive trend monitoring of pilots' resilient adaption to potential or actual changes in the weather.

An operationalization of the fecor with leading indicators classified in theoretically sound main- and subcategories allows for developing theory based models. When these models reflect the normal functioning of a system at the sharp end, they describe in a comprehensible manner which activities and prerequisites are critical for creating and sustaining resilience and hence for being proactive. Furthermore, a questionnaire for reliable measurement of the fecor facilitates resilience management by monitoring resilience specific activities (behavior, methods, outcomes) and critical prerequisites.

Using the tested questionnaire on a regular basis (e.g. twice a year) supports the identification of resilience-relevant trends in the measured scales. These trends need to be discussed and interpreted by representatives from the pilot corps and the Flight Safety Department. Such, problematical or undesirable developments can be recognized and appropriate, proactive measures can be taken. At a later stage the intended impact of the measures taken can statistically and qualitatively be evaluated. This proactive management of resilience helps an organization to sustain and to promote resilience. Furthermore, more practical experiences with this way of managing resilience supports the resilience community in developing and implementing target-oriented processes of resilience management in a complex, high-risk organization.

REFERENCES

Dekker, S., Hollnagel, E., Woods, D. & Cook, R. (2008). *Resilience Engineering: New directions for measuring and maintaining safety in complex systems.* retrieved from https://www.msb.se/Upload/Kunskapsbank/Forskningsrapporter/Slutrapporter/2009%20Resilience%20Engineering%20New%20directions%20for%20measuring%20and%20maintaining%20safety%20in%20complex%20systems.pdf [04.01.2015].

Hollnagel, E. (2012). A Tale of Two Safeties. *The Resilient Health Care Net*. retrieved from http://www.resilienthealthcare.net/A_tale_of_two_safeties.pdf [04.01.2015].

Hollnagel, E. (2014). Resilience engineering and the built environment. *Building Research & Information, 42*, (2), 221 - 228.

Hollnagel, E., Pariès, J., Woods, D. D. & Wreathall, J. (2011). *Resilience Engineering in Practice - A Guidebook.* Farnham, UK: Ashgate.

UNDERSTANDING RESILIENCE IN FLIGHT OPERATIONS

Arthur Dijkstra
ADMC, Kooikerboog 7 Nederhorst den Berg, Netherlands
Arthur@ADMC.pro

Abstract

An effective Safety Management System requires high variety feedback from flight operations. Current methods for gathering operational data are not suitable for personal, contextual, opinions and views of the people at the sharp end of flight operations. Operational risk mitigation and the handling of disturbances is an essential quality of the flight crew. FlightStory supporting operational feedback, makes the pilots more part of a human sensor system to improve safety. The management of flight operations can learn how actual practices shaped safe performance under goal constraints and resource limitations. FlightStory provides a high variety feedback system. The pilots have access to an app on their iPad to submit their stories. Relevant aspects of Resilience Engineering and the Viable System Model are used to find patterns in effective handling of all types of events, not only safety incidents. Remarks in FlightStories show pilots appreciate the method and wish to share their experiences. The stories show how uncertainty, ambiguity and complexity can play a role in normal pilot event handling and how resilience is realised.

1 INTRODUCTION

Safety is a critical variable for the survival of an airline. In times where the competition is fierce, the impact of regulations is strong, traffic is increasing and technology is more and more connected, safety management is demanding. The already high level of safety of aviation requires new methods for further improvements in safety.

FlightStory is such a new method. It builds on the related fields of cybernetics, systems theory and resilience engineering. A high variety channel from the flight operations back to the organisation is needed to specify the gap between Work As Imagined,(WAI) and Work As Done (WAD) (Wears, 2015). Hollnagel (2014) describes that according to the safety-II principle all events should be evaluated, not just the undesired outcomes. FlightStory provides pilots a way to communicate their experiences and explain how system perturbations affected flight operations.

Safety-II and Resilience Engineering (RE) as described in Hollnagel (2007) are not yet part of the vocabulary of current Safety Management System (SMS) methods. Most of today's SMSs focus is put on hazard identification, mitigation and the failures that occurred. Current practices for data collection from flight operations consist of Flight Data Monitoring (FDM), the monitoring of about 160 flight parameters, Air Safety Reports (ASR), reports written by pilots giving factual data about a safety related event, and legally required flight inspections executed by flight inspectors. These practices have not changed a lot over the last 20 years except for the introduction of voluntary Line Oriented Safety Audit (LOSA) (ICAO 2002). During LOSA a trained observer fills out a LOSA form about how threat and errors were managed and what kind of errors or violations were made. The LOSA form and the introduction of an interpretative layer (the observer) is problematic given the complexity of flight operations. Page (2010) states that complexity requires a diversity of perspectives. Similarly trained observers and predetermined scoring forms do not increase the number of perspectives. The transduction of variety (Beer 1985) by the LOSA form and the observer reduce the maximum feedback variety.

Amalberti (2001) suggests that standard reports become ineffective in ultra-safe systems. FlightStory is an instrument for pilots to express themselves. It allows them to give their view of a safety related event and allow them to express how they (almost always) successfully dealt with the event. Operational risk mitigation and the handling of disturbances is an essential quality of the flight crew. FlightStory makes the pilots more part of a human sensor system so the organisation can create more information about itself in order to manage itself more effectively (Beer 1972). This can increase the requisite variety of the Safety Management System (Ashby 1958).

1.1 Aims and objectives

FlightStory should provide insights in how pilots disturbances and balance safety with other goals during normal, everyday flight operations. Their stories, opinions and beliefs can provide meaningful insights and help bridge in the gap between WAI and WAD. FlightStory analyses should provide directions for management interventions to further improve the resilience of flight operations.

2 METHOD

As an initial test, FlightStory was made available to the flight instructor pilots only. This group consists of about 200 pilots who perform regular flight, route and simulator training and checking. About half of the group is short haul pilots (flights less than 4 hours) and the other half is long haul pilots (normally longer than 4 hours).

This sample of pilots is representative for the total group of pilots since they operate on regular line flight with regular (no training) colleagues.

2.1 Data collection

FlightStory was built as an HTML5 single page app. Capable of working while in flight, not connected to the internet. The app has a mobile user interface suitable for usage on an iPad. After a FlightStory was completed by a pilot the answers were sent by email to the safety office following the same route as electronic safety reports. In the safety office the answers in JSON format are extracted from the email and stored in a secure database. The instructor pilots were invited by their training managers to share their experiences by FlightStory. In a letter to the instructor pilots the purpose, the installation procedure and working of the app were explained.

2.2 Experiment design

FlightStory is inspired by Sensemaking and Storytelling. This field of research can be traced back to the 1970's (Dervin 1983). Weick and Sutcliff (1999, 2005) applied Sensemaking concepts to understand how organisations develop and maintain high reliability in complex environments. Kurtz and Snowden (2003) included explicitly complexity theory concepts to their Sensemaking approach. Complexity theory assumes that it is not a priori possible to know all the issues and relations in a complex system. Therefore open questions are needed to collect relevant data as opposed to closed questions which assume the issues and relations are known. Standard ASRs that are currently filled out by the pilots when a safety event has occurred, have only boxes to tick and a field for a factual event summary. The pilots view on the event is not systematically collected in ASR. During analysis for SMS purposes the ASRs are categorised and grouped to find trends. This data treatment disregards the contextual data. Combined FlightStory and ASR, data remains contextual and can be analysed differently.

For this experiment the FlightStory will be an extension of the ASR. The narrative, describing the operational experience, provides qualitative data. The pilots indicates his view via the triangles and selection boxes. The quantitative data is used to find patterns in the data. The qualitative data is used to support understanding of the patterns found. The FlightStory form consists of three parts.

The first part of FlightStory starts by asking the pilot an open prompting question (such as: Please describe your experience in a way other pilots can learn from your event.") Here the pilot provides his narrative of the event. The first part also gathers some personal data such as function, experience and emotional impact (this is an indicator for the impact of the event). The pilot is also asked to assign a personal judgement to the risk level of this event. This allows comparing SMS assigned risk levels done by the safety office and the views of the pilots.

The second part of the FlightStory form has ten tri-arcs covering a mix of relevant RE and Viable System Model (Beer 1984) concepts. The concepts are placed in a triangle or ternary plot as used by Keidel (1995) and Allen (2007). In FlightStory these shapes are called tri-arcs. This shapes provides a better geometry since the opposite arc segment from a corner has equal distance to this corner. This is not the case in triads.

The distance between the concepts in the tri-arc allows the reporter to weight his judgement. The distance from the selection point in the tri-arc to each concept corner is a value indicative for the significance of the concept for the specific question. In this case the tri-arc provides a way to indicate what was supportive to handle the specific situation: Standard Operating Procedures, Advice from other such as Flight Dispatch, Maintenance support or Improvisation. In the example above more Improvisation was used than Standard Operating Procedures and Advice. A remark can be added. A mark in the middle would indicate all three features are equally important. If none of the labels are applicable one can choose to check the 'Not Applicable' box.

Research (Snowden 2011) has shown that respondents using the tri-arcs used more time and consideration where to place the mark than when two point scales are used. A tri-arc signifying space is richer than a two point scale and also more two point scales than tri-arcs would be required to get the same amount of data. A tri-arc provides a way to indicate which or how trade-offs were made. Pilots can add remarks to their answer.

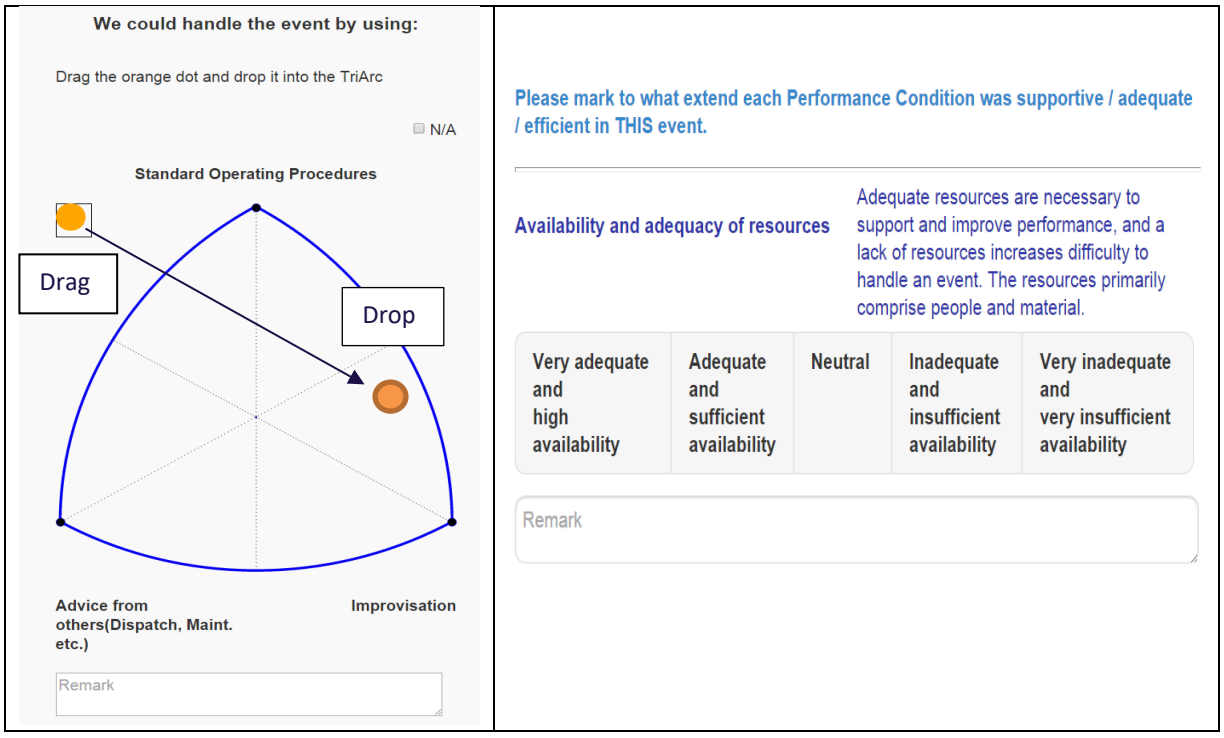


Figure 1 Left: A tri-arc showing concepts at each corner. Right: A question with radio buttons about Operational Performance Conditions

Snowden in Mosier (2011) suggests two options to design relevant labels for the tri-arcs. One is to search for cultural established organisational constructs, the other is a researcher designed set related to the aim of the research. The labels provide references for the respondents and help to signify their judgement about the reported. The following steps were used to specify the concepts labels:

1. Identify the concepts in the field of safety, safety management and resilience by clustering subjects, behaviours, decision points, etc. from a priming set of narratives and literature. Choose the key concepts that relate strongest to the project, here resilience.
2. For each key concept create a triad with balanced negative or positive labels, the idea is to force trade-offs.

The concepts are based on a review of Resilience Engineering (RE) (Hollnagel et.al.2011) and Management Cybernetics literature (Ashby 1956, Beer 1972). Both fields of theory align well as argued in Dijkstra (2007). The following key concepts were selected and used in the questions.

1. System identification, what are the essential variables, which could be affected.
2. What was the source of the disturbance
3. How complex was the event
4. Response characteristics
5. System dynamics
6. Core competencies (ICAO 2013)
7. VSM related concepts, the four essential abilities
8. System dynamics, time, margin, fall back options.
9. Learning system

The ICAO Core Competencies answers are useful for the Alternative Training and Qualification Program (ATQP) development. FlightStory provides feedback to update an understanding on how the core competencies are applied in actual cases. This question was added after a discussion with the Head Of Training of the airline.

The third part of the FlightStory form contains the Common Performance Conditions (CPC) as developed by Hollnagel (1998). The CPC can be rated on a scale for their supportiveness for handling the situation. CPCs can be viewed as the factors that are managed by the airline organisation, through the SMS, that shape the performance of their flight operations. The combination of CPC rating and resilience safety performance can provide and increased understanding of how to engineer a more operational resilience.

2.3 Summary

FlightStory accommodates high variety feedback from flight operations feedback on issues related to: the pilots view and opinion, RE concepts, pilot training and operational performance conditions.

3 RESULTS

Confidentiality agreements prevent publishing details of stories. The provided examples and excerpts in this paper are considered representative for normal work in flight operations of any airline. Outsiders normally have no access to these insiders stories. This publication provides some insights which in not unique for the particular sources of these stories.

3.1 Reporting rate

After the experiment ran for 6 months 25 FlightStories were submitted. Ten FlightStories were short haul related and 15 long haul. A submission per flight rate is hard to determine since individual pilot schemes, showing actual flight and simulator working periods are not available for this research. A rough estimate would be based on the following assumptions: pilots perform simulator and flights on about a 50/50 rate. Thus 3 months of flight means for a short haul pilot about 100 flights. For 100 pilot this totals to 10000 flights. This makes the response rate in the order of 1 in 1000 flights for short haul. 100 long haul pilots fly about 2500 flights in three months. Hence the response rate is in the order of 1 in 150 flights.

3.2 Analysis method

A specific FlightStories analysis tool is in development. This analysis is based on a simple spreadsheet overview.

3.2 Story titles

The story titles already provide a sense for the topics that were addressed in the FlightStories. Some examples of story titles: “50 shades of grey”; “Insufficient wingtip clearance during taxi-out?”, “Always Be Prepared”, 'Acceptability' vs 'accountability'.

Topics such as uncertainty, ambiguity and trade-offs can be inferred from these titles. These titles seem to refer complex issues, the areas where resilience and operator expertise become relevant.

3.3 Excerpts of stories

Each flight was without incident or specific threat to safety. These were normal operations as they are regularly encountered. Normally these events are shared among pilots and only factually reported in standard safety reports and not with the aim to share learning with colleagues.

1. When the weather conditions are outside the limits for the autopilot:

“Also we encountered a few times an updraft. This updraft with the tailwind put us high on glide, while holding power at idle and using full speed brakes. At about 10500' I disconnected the AP and continued manually, still the same turbulence and speed fluctuation. Also still holding above the glide path. At around 1000' AGL we were fully configured for landing, still above the glide but correcting this time, I decided to continue and wait for the 500' call, we were VFR and had lots of positive energy. AT 500' we were on glide, the air was a little more stable, only some overspeed.”

CPC Crew Resource Management was rated as very efficient and training and experience was rated as very adequate. An Air Safety Report was filed and no Flight Data Monitoring events were triggered. After the flight the pilot felt “relieved”

2. Disturbances, non-standard operations and delay:

”Apart from above mentioned circumstances, worth noting is that during the sequence of events, already being out-of-the-ordinary, cockpit split several times, as different parties (ATC, ground staff, marshaller, AMT and crew/pax) require attention and once considered safe, losing as little time as possible, to guarantee scheduled arrival time, the biggest threat seemed to continuously keep cockpit crew in the loop, and to adhere to SOP's to guard all barriers for safe operation. Making very short 'recaps' before second pushback, before second taxi-out and before take-off helped to minimize this threat. Luckily, we were fortunate that -even with LSF (low speed flying)- we would still arrive on time after 45' delay, so time pressure was minimal.”

CPC Human Machine Interface and Operational support was rated as Unsupportive. An Air Safety Report was filed and no Flight Data Monitoring events were triggered.

3. Winter operations:

“I was kind of surprised! I could suddenly "feel" my right hand touching my right knee as it should be. Or not? We had started that morning very early with "the Europe Works": no drinking water in tanks, de-icing and a slot time, precipitation now and then, water in tanks but no pressure, should we take extra fuel, "What's that a minimum fuel uplift?", boarding and one pax missing, etc. etc. After having been de-iced and made our slot, we had an uneventful t/o for our relatively short flight to LHR, somewhat delayed of course.”

For this flight no ASR was written (maybe because a FlightStory was filed) and no FDM events were triggered. The pilot judged the event as medium risk but since no ASR was written a discussion about SMS risk and perceived pilot risk was impossible. This example is maybe indicative for the pilot’s desire to share an experience which cannot be shared via standard reporting such as the ASR. The pilot felt worried after the event.

3.4 Pilot responses on the FlightStory app

“A way to improve safety and awareness without the need for an ASR.”

“I can give more background information, which is important with human factors.”

“I have to get used to the tri-arcs. But I can imagine it can give valuable information to fill them in, since you are forced to think about aspects you didn't think of beforehand.”

“Too labour some”

“Good plan, but should be more simple. Terms used too theoretical for pilots.”

“This is important! Sharing brings this experience to all! We can all benefit to this report. I also learn from it by sending the report.”

3.5 Summary

The pilot responses indicate a desire to improve safety by sharing and learning. The stories and their titles indicate trade-offs and goal conflicts, the typical arena where resilience engineering is applicable. Event descriptions which contain context and participants opinions show insights that would otherwise be unavailable for safety management purposes.

4 DISCUSSION

The response rate is still below the desired rate. Pilots stated that a rate of about 1 FlightStory in 10 flights should be achievable. The time and effort to fill out a FlightStory should be outweighed by the benefit pilot perceive from sharing the stories. A promotion campaign will be started.

The analysis tool that is in development together with more submitted FlightStories will help to find patterns. These are desired to understand effective strategies and enable support for resilience via e.g. training and flight operations design.

FlightStory provides descriptions of events from the pilots perspective. These insights are normally not systematically available by other means. The stories provide e.g. issues to discuss during pilot training. Especially new captains can learn to monitor, anticipate and respond from discussing these FlightStory events.

Initial draft results have only just been shared with some managers of the flight operations department. Their reaction is positive as expressed by their desire to get more results in a monthly report and to support the promotion campaign.

5 CONCLUSIONS AND CONCLUDING REMARKS

FlightStory is a new way of building a high variety feedback from flight operations to flight operations management. The stories can also be shared among pilots to learn from others’ experiences. Therefore expectations by pilots and managers about FlightStory are high. Analysis shows that new information is collected for safety management, operational management and fellow pilots. The methodology has been effective in other domains(Deloitte 2010). It is expected that all pilots in the company will be invited to share their operational experiences via FlightStory to increase the understanding of the gap between WAI and WAD. Some remarks have resulted in improvements of the app and feeding the stories back to pilots will start coming months. The airline supporting this project is taking a step forward in developing effective safety management methods.

REFERENCES

Allen, G.D. & Goldsby, D.S. (2007). Using technology to make new assessment instruments, Proceedings of the 18th International Conference on Technology in Collegiate Mathematics. Boston: Addison-Wesley

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. Safety science, 37(2)

Ashby, W. R. (1958). Requisite variety and its implications for the control of complex systems. Cybernetica, 1.

Beer, S. (1984). The viable system model: Its provenance, development, methodology and pathology. Journal of the operational research society.

Deloitte, (2010) Mining Safety a Business Imperative.

Dervin, B. (1983). An overview of sense-making research: Concepts, methods, and results to date. The Author.

Hollnagel, E. (1998). Cognitive reliability and error analysis method (CREAM). Elsevier.

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2007). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

Keidel, R. W. (1995). Seeing organizational patterns: A new theory and language of organizational design. Berrett-Koehler Publishers.

ICAO (2012) Manual of Evidence-based Training, Doc 9995.

Mosier, K. L., & Fischer, U. M. (Eds.). (2011). Informed by knowledge: Expert performance in complex situations. Psychology Press.

Page, S. E. (2010). Diversity and complexity. Princeton University Press.

Stafford, B. (1985). Diagnosing the system for organizations. John Wiley & Sons

Wears, R. L., Hollnagel, E., & Braithwaite, J. (Eds.). (2015). Resilient Health Care, Volume 2: The Resilience of Everyday Clinical Work. Ashgate Publishing, Ltd..

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. Organization science, 16(4).

EXPERIENCES FROM AVIATION: DESIGNING AND DEVELOPING ORGANISATIONS

AN OVERVIEW OF AGILITY AND RESILIENCE: FROM CRISIS MANAGEMENT TO AVIATION

Rogier Woltjer 1, Björn J.E. Johansson 2, and Peter Berggren 3
Department of Information and Aeronautical Systems, Swedish Defence Research Agency FOI, P.O. Box 1165, SE-581 11 Linköping, Sweden
1 rogier.woltjer@foi.se, 2 bjorn.j.e.johansson@foi.se, 3 peter.berggren@foi.se

Abstract

The concepts of agility and resilience both focus on the management of complex safety- and security-critical operations in terms of adaptability of operations in the face of change and unforeseen circumstances. After providing an overview of key concepts associated to resilience and agility from Resilience Engineering (RE), disaster management, crisis management and military command and control (C2) perspectives, this paper identifies research tensions, opportunities for cross-over of research foci, and challenges for the successful practical application of both agility and resilience. Resilience from the military C2 agility perspective seems to be mostly related to rebound or recovery, and is thus a distinctly different from how resilience is used in RE and disaster management. The other enablers (responsiveness, versatility, flexibility, innovativeness, adaptability) of agility and C2 agility, and the resilience perspectives of graceful extensibility and sustained adaptability, seem promising for innovation in aviation, pointing research to organizational and design principles to support adaptation and cope with surprise. Associated research questions applied to aviation are exemplified.

1 INTRODUCTION

The concepts of agility and resilience have a similar bearing on the management of complex safety- and security-critical operations in terms of adaptability of operations in the face of change and unforeseen circumstances that are not fully avoidable. Both fields have emerged as a reaction to earlier, mechanistic/tayloristic attempts to safeguard against failure. Agility is a term used in the literature on organizational theory (Holsapple & Li 2008; Spaans, Spoelstra, Douze, Pieneman & Grisogono, 2009) military command and control (Alberts, 2007, 2011; NATO STO SAS-085, 2013) and crisis management (Farrell, Baisini, Belanger, Henshaw, Mitchell & Norlander, 2013). Resilience has been applied in a number of social and physical sciences, such as ecology, clinical psychology, materials science, and engineering. Resilience as used in Resilience Engineering (RE; Hollnagel, Pariès, Woods, & Wreathall, 2011; Hollnagel, Woods, & Leveson, 2006) has its basis in cognitive systems engineering (Hollnagel & Woods, 1983, 2005), human factors, and safety science. Disaster management literature has also used the concept of resilience for some time (Boin, Comfort, & Demchak, 2010; Manyena, 2006). Several common definitions of the two concepts are at least partially overlapping, yet they stem from rather different conceptual backgrounds and problem areas. Both approaches do however share that they have emerged as a consequence of growing complexity and unpredictability in the type of stakeholders' activities.

In this paper, research tensions, opportunities for cross-over of research foci, and challenges for the successful practical application of both agility and resilience in relation to associated research disciplines are identified. With the help of the concepts of resilience and agility various research communities connected to different fields of practice aim to enhance socio-technical systems' adaptability and pro-activeness in coping with unpredicted events. However, these concepts are used in vastly different ways. Not addressing research tensions and opportunities for cross-over of advances between different fields and research communities might hinder the progress made towards the goal of these research endeavours, which is to improve operational management of complex systems in practice. A focused discussion of research progress of agility and resilience and its practical implications is therefore relevant and needed. This paper attempts to advance this discussion and provide implications for research on agility and resilience in aviation.

2 THE FOCI OF RESILIENCE IN RESILIENCE ENGINEERING

Resilience has been defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions." (Hollnagel, 2011a) (p. xxxvi). This definition reflects the need to not only reactively adjust after disturbances are observed but also when they are anticipated to occur. Adjusting performance with respect to disturbances but also subtle changes is essential, as fluctuations in working conditions may coincide and combine

to hazardous situations due to complexity and intractability. RE emphasises the need to see the multiple goals that the core business aims to achieve, which is hardly only safety but often also productivity, security, environmental sustainability, etc. RE recognizes that not all conditions can be expected and prepared for beforehand, and that unexpected conditions will at some point occur. In order to achieve resilience, four interrelated and interacting abilities have been suggested: anticipating (knowing what to expect), monitoring (knowing what to look for), responding (knowing what to do), and learning (knowing what has happened) (Hollnagel, 2011b).

Articulating the importance of unexpected conditions in Resilience Engineering, another definition focuses on the situations that go beyond what the organisation or system has prepared for: ”the ability to recognize and adapt to handle unanticipated perturbations that call into question the model of competence, and demand a shift of processes, strategies and coordination” (Woods, 2006) (p. 22). Recently Woods outlined four uses of the concept of resilience: as rebound, as robustness, as graceful extensibility when surprise challenges boundaries, and as a network architecture that can sustain the ability to adapt to surprise (named Resilience-1 to 4) (Woods, in press).

3 THE FOCI OF RESILIENCE IN DISASTER MANAGEMENT

The emergency and disaster management literature has acknowledged the importance of the concept of resilience for some time (Manyena, 2006). Modern crises may be characterised by an increase in coupling and complexity, which makes prevention, mitigation, and preparation very challenging (Boin et al., 2010). A definition of resilience in the disaster management strand of research is: “Resilience is the capacity of a social system (e.g., an organization, city, or society) to proactively adapt to and recover from disturbances that are perceived from within the system to fall outside the range of normal and expected disturbances” (Boin, Comfort, & Demchak, 2010, p. 9). Besides similarities in proactivity, a tension can e.g. be found between the inclusion of expected events (as in Hollnagel’s (2011a) definition above) and the restriction of resilience to the unexpected and not-prepared-for, as in Boin et al.’s (2010) as well as Woods’ (2006) definitions of resilience.

Research tensions and challenges for the definition of resilience in disaster management in relation to related disciplines have been described in three aspects (Boin et al., 2010): (a) the moment of resilience (response/recovery after the event and/or adaptation beforehand); (b) to which event severity it applies; and (c) the state of return that resilience applies to (returning to a situation similar to before the event, make the system function again, or making it stronger than it was before).

4 THE FOCI OF (C2) AGILITY

The concept of agility is related to the concept of resilience in the sense that there is a common focus on adaptation of the management of command and control processes not only after a certain disturbance or event but also in a proactive manner. This paper focuses on agility and C2 agility as defined by and in connection to the NATO STO SAS task-groups (NATO STO SAS-065, 2010; NATO STO SAS-085, 2013) whereas other definitions and uses of the term exist.

Agility is developed from a problem space of command and control characterised by time pressure, uncertainty, and risk, in the face of complexity. Similar to the development of resilience engineering described above, military operations have become so complex that effective command and control and performance in military operations should be described as emergent properties of the behaviour of MTO-systems (Man-Technology-Organization), rather than simple cause and effect relationships. Similarly to the Resilience Engineering and Safety-II perspectives, agility is about “maintaining success in light of changed or changing circumstances” (Alberts, 2011) (p. 66). It includes both passive–active and reactive–proactive components. Alberts concludes with the following definition: “Agility is the ability to successfully effect, cope with, and/or exploit changes in circumstances” (Alberts, 2011) (p. 190) and (SAS-085, 2013) (p. 54).

Agility is a multi-faceted concept which includes the following components: responsiveness, versatility, flexibility, resilience, innovativeness, and adaptability (Alberts, 2011) (p. 204). Resilience is subsequently described as providing a system with “the ability to repair, replace, patch, or otherwise reconstitute lost capability or performance (and hence effectiveness), at least in part and over time, from misfortune, damage, or a destabilizing perturbation in the environment” (Alberts, 2011) (p. 217). Apart from the adversary as an obvious source of perturbations in a military environment, acts of nature and inevitable results of complexity are also mentioned as sources, providing overlaps with the disaster management and resilience engineering fields respectively. Resilience is in this description however more in line with resilience as described in for example physics, meaning the ability to bounce back to an earlier performance level after a disturbance, essentially a passive capacity. In contrast, some authors in the Resilience Engineering and disaster management field, see pro-active adaptability

in anticipation of degradation as part of resilience. Adaptability is another overlapping theme, although here it is seen as a part of agility that is related to but separate from resilience.

The NATO SAS-085 "C2 Agility and Requisite Maturity" further develops this into a C2 Approach Space and a conceptual model of C2 agility (NATO STO SAS-085, 2013). While agility, as such, describes the ability of an entity to cope with a complex and dynamic environment, C2 agility describes the ability of the unit to adapt its way of organizing work to fit the problem at hand. To be C2 agile is thus a property describing to what extent the C2 organization can adapt its way of working to the current situation in terms of dissemination of information, allocation of decision rights and patterns of interactions (organization and structure). A fundamental hypothesis in the NATO STO SAS work has been that each type of situation/problem/mission has its own ideal point in the command and control approach space – no organization type is thus perfect for all kinds of missions/situations. Similar observations have been made in the studies of High Reliability Organizations:

> "The navy has managed to balance the lessons of the past with an openness to change and create and organization that has the stability and predictability of a tightly run hierarchy but that can be flexible when necessary…… Depending on the demands of the situation, people will organize themselves into different patterns. " (Pool, 1997, p. 42-44).

5 IMPLICATIONS FOR AGILITY AND RESILIENCE RESEARCH IN AVIATION

This section discusses some of the components of the definitions outlined above from military and crisis management to identify research questions for aviation. First, the need for aspects of agility and resilience may be identified as part of the International Civil Aviation Organization (ICAO) definition of Air Navigation Service (ANS) expectations, which are highlighted to make the point that the concepts seem to suit well to the ANS operational environment. Second, examples of research questions are derived from some of the highlighted definitions as a research agenda.

As an example of how central and important the presented concepts are to Air Traffic Management (ATM), the expectations of ANS flexibility, and capacity have bearing on agility and resilience. *"Flexibility* addresses the ability of all airspace users to modify flight trajectories dynamically and adjust departure and arrival times, thereby permitting them to exploit operational opportunities as they occur." (ICAO, 2005, p. D-2). The expectation of flexibility thus includes exploiting opportunities, a central concept in agility. The expectation of *Capacity* expectations address resilience explicitly and links several high-level expectations to each other: "The ATM system must be resilient to service disruption and the resulting temporary loss of capacity" (ICAO, 2005, p. D-1). Improving the ability to exploit opportunities and be resilient to service disruption are thus in the interest of the aviation system, and theoretical frameworks that enhance these abilities may be employed to do so.

As a step in this direction, Table 1 includes a number of the concepts as part of the agility and resilience literature and their definitions, and identifies applied aviation research questions for further research.

Table 1. Agility (A) and resilience concepts, with example research questions applied to aviation

Concept	Definition	Aviation agility/resilience research question examples
Responsiveness (A)	The ability to react to a change in the environment in a timely manner (NATO STO SAS-085, p. 204)	How can a change be detected by different stakeholders and roles at different levels? What response is required? What are the *criteria* for a successful response (e.g. separation maintained, safe landing, minimize economic loss), and *how* (indicators) and *when* (immediate, delayed) can these be assessed? How does response at the *sharp* (pilots, controllers (ATCOs), maintenance engineers) and *blunt* ends (safety/crisis managers, middle/top management) interact and how are they interdependent? Is a collective response by stakeholders (several ANSPs, several airlines, ANS Provider-airport-airline, etc.) expected/beneficial?
Versatility (A)	The ability to maintain effectiveness across a range of tasks, situations, and conditions (NATO STO	How are competencies and tasks distributed among operators (e.g., controllers being certified on various clusters of area control sectors, or both tower/terminal control; pilots with multiple type ratings; engineers with crisis management roles)? How can resources be made available and shared so that

	SAS-085, p. 205)	stakeholders' task coordination is facilitated (e.g., airline and manufacturer sharing crisis facilities)?
Flexibility (A)	The ability to employ multiple ways to succeed and the capacity to move seamlessly between them (NATO STO SAS-085, p. 203)	Which alternative courses of action can be taken to achieve goals (e.g., are several procedures available so that the choice of procedure is not obvious)? How do alternative courses of action intertwine? How do operators know when to switch strategy (e.g., how can ATCOs and pilots be prepared generally to identify when a procedure in an unusual situation is taking too much time to complete)?
Resilience (A)	The ability to recover from or adjust to misfortune, damage, or a destabilizing perturbation in the environment (NATO STO SAS-085, p. 204)	What strategies and resources are necessary and available to recover to a normal state? What is the normal state to recover to (e.g., in terms of flight delays, re-routings, ANS capacity levels)? Similar to Rebound (R-1), below.
Innovativeness (A)	The ability to do new things or the ability to do old things in new ways (NATO STO SAS-085, p. 204)	How can operators be encouraged to come up with new ways to achieve goals? Are alternative resources available to use in innovation of ways of working (e.g., particular expertise, maps, break-out rooms, simulation resources)? When are new approaches necessary and how do operators identify this?
Adaptability (A)	The ability to change the organization and/or work processes. (NATO STO SAS-085, p. 199)	What mechanisms are in place for changing organization and/or processes (e.g. prepared crisis-mode organization responsibilities and communication channels)? How can different levels of the organization be prepared for unexpected and new changes in work processes?
Resilience cornerstones	Monitor, respond, learn, anticipate	See Resilience Analysis Grid (RAG; Hollnagel, 2011b)
Rebound (R-1)	Rebound (Woods, in press)	See Resilience (A) above, as resilience from the agility perspective is defined as recovery from perturbation.
Robustness (R-2)	"increased ability to absorb perturbations" (Woods, in press, p. 2)	Woods (in press) argues that robust control works for well-modeled and well-understood situations, but that increasing robustness may decrease resilience (R-3/4). Thus it is relevant to ask which situations are modeled and handled using the processes and system designs in place. For example, safety assessment techniques in both air traffic management and aircraft manufacturing model a large number of risks. R-3 and R-4 (below) would ask how to cope with the surprise situations that are not covered by these methods, rather than relying on that all these anticipatory processes fully specify all future situations.
Graceful extensibility (R-3)	"resilience as the opposite of brittleness, or, how to extend adaptive capacity in the face of surprise" (Woods, in press, p. 3)	This perspective on resilience asks "how do systems stretch to handle surprises?" (Woods, in press, p. 3). Thus it is relevant to ask what aspects of a situation are regarded as surprises, how do controllers and pilots identify surprise, and what strategies can be identified that operators and organizations use to adapt (see Rankin et al. 2013, for an attempt in describing some of these issues for flight crews).
Network architectures for sustained adaptation (R-4)	"the ability [to] manage/regulate adaptive capacities of systems that are [and are part of] layered	The air traffic system arguably develops more and more towards increased interdependency between nodes in a layered network. ATM units and aircraft become more interconnected (e.g. through trajectory management) and aviation stakeholders are more linked than ever before (e.g.

	networks […] to produce sustained adaptability" (Woods, in press, p. 4)	through collaborative decision making). Questions from this perspective (Woods, in press) ask how architectures of these networks, and design principles and techniques (see Woltjer et al., in press, for an attempt in this direction for ATM) can support adaptation at and between layers over time, and how this property can be assessed.

6 DISCUSSION

Agility, and C2 Agility, thus shares some concepts with resilience, primarily in term of their aims. Both resilience and agility consider adaptive capacity as the primary way to cope with the kind of events that emerge from the complexity of today's challenges. They both consider learning as an important source for improving the ability to cope with challenges, but they also recognise the need to be able to cope with what cannot be anticipated. However, there are some important distinctions too. Firstly, resilience engineering, and safety in general, does not cope with an intelligent enemy and therefore does not need to "exploit changes in circumstances" in that sense – it is enough to "sustain required operations". However, an issue that is more prevalent in aviation, and that military is affected by but in a less distinct manner, is the economic pressure in the highly competitive aviation environment. The "exploit changes in circumstances" aspect of agility could provide a contribution here, linking business continuity and interactions of these aspects with crisis management and safety management aspects in aviation stakeholders. Also, the expectation of flexibility in the ATM system clearly points to the need for exploitation of operational opportunities, for example in order to provide efficiency in traffic flows.

Further, agility focuses largely on adaptive capacity in terms of C2 (by utilizing the C2 approach space and the concepts of C2 maturity and C2 maneuverer agility), which would translate to "organization" or "management" in the industrial domain. Resilience engineering is not specific in its view on organization/management and lacks a theoretical construct for discussing how management and organization can or should adapt to changing circumstances. The concept of "layered network architectures for sustained adaptation" (Woods, in press) seems a step in this direction and highlights a similar concern for organizational and design principles to support adaptation, which may be developed further for aviation translating the C2 agility approach space to aviation.

Resilience from the agility perspective described seems to be most related to "rebound" or "recovery", and is thus a distinctly different from how resilience is used in Resilience Engineering and disaster management. Robustness and recovery aspects have a longer history in aviation so that the other enablers of agility and the perspectives of graceful extensibility and sustained adaptability seem more promising for innovation. Associated research questions have been exemplified for aviation (see Table 1). Other research tensions identified include whether expected conditions should be included in the concept of resilience, and to which extent anticipation is part of resilience/agility.

Possibly due to Resilience Engineering's roots in mainly cognitive systems engineering and reactions to traditional human factors and safety, the debate of how Resilience Engineering can contribute to these operational practices often focuses on discussions as reactions to traditional safety and human factors paradigms. This paper has aimed to broaden this discussion and argues for the consideration and relevance of a number of concepts and ideas developed under the label "agility", and how these may contribute to improving operational realities in ways congruent to the ambitions of resilience engineering. In particular, these concepts may broaden the discussion of resilience from safety to business continuity concepts such as seizing opportunity and exploiting circumstances, and clarify the multifaceted concept of adaptability of organizational features.

Acknowledgements

This paper is based on work partly funded by the EU H2020 Mobility for Growth programme in the project Future Sky Safety, P5 Resolving the Organisational Accident, WP5.4 Agile Response Capability. The views and opinions expressed in this paper are those of the authors and are not intended to represent the position or opinions of the Future Sky Safety consortium or any of the individual partner organisations.

REFERENCES

Alberts, D. S. (2007). *Agility, Focus, and Convergence: The Future of Command and Control*. The International C2 Journal, 1(1). 1-30.

Alberts, D. S. (2011). *The Agility Advantage: A Survival Guide For Complex Enterprises and Endeavors*. USA: DOD CCRP. Retrieved from http://dodccrp.org/files/agility_advantage/Agility_Advantage_Book.pdf .

Boin, A., Comfort, L. K., & Demchak, C. C. (2010). The rise of resilience. In L. K. Comfort, A. Boin, & C. C. Demchak (Eds.), *Designing Resilience: Preparing for Extreme Events* (pp. 1–12). Pittsburgh, PA: University of Pittsburgh Press.

Farrell, P. S. E., Baisini, C., Belanger, M., Henshaw, M., Mitchell, W., & Norlander, A. (2013). SAS-085 C2 Agility Model Validation Using Case Studies. In *Proceedings of the 18th ICCRTS*, Alexandria, VA, June 19-21. Washington, DC: DoD CCRP.

Hollnagel, E. (2011a). 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). Aldershot, UK: Ashgate.

Hollnagel, E. (2011b). Epilogue: RAG – The Resilience Analysis Grid. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), *Resilience Engineering in Practice: A Guidebook* (pp. 275–296). Aldershot, UK: Ashgate.

Hollnagel, E., Pariès, J., Woods, D. D., & Wreathall, J. (Eds.). (2011). *Resilience Engineering in Practice: A Guidebook*. Aldershot, UK: Ashgate.

Hollnagel, E., & Woods, D. D. (1983). Cognitive systems engineering: New wine in new bottles. *International Journal of Man-machine Studies, 18*(6), 583-600.

Hollnagel, E., & Woods, D. D. (2005). *Joint cognitive systems: Foundations of cognitive systems engineering*. CRC Press.

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

Holsapple, C. W., & Li, X. (2008). Understanding Organizational Agility: A Work-Design Perspective. In *Proceedings of the 13th ICCRTS*, Seattle, WA, June 17-19. Washington, DC: DoD CCRP.

ICAO. (2005). *Global Air Traffic Management Operational Concept*. International Civil Aviation Organization.

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters, 30*(4), 433–450.

NATO STO SAS-065 (2010). *NATO NEC C2 Maturity Model* (CCRP Publication Series). Washington, DC: DoD CCRP.

NATO STO SAS-085 (2013). *C2 Agility – Task Group SAS-085 Final Report* (STO Technical Report STO-TR-SAS-085). Brussels, Belgium: NATO Science and Technology Organization.

Pool, R. (1997). When failure is not an option. *MIT's Technology Review, 100*(5), 38-45.

Rankin, A., Woltjer, R., Field, J., & Woods, D. (2013). "Staying ahead of the aircraft" and Managing Surprise in Modern Airliners. In *Proceedings of the 5th Resilience Engineering Association Symposium* (pp. 209–214). Soesterberg, NL: Resilience Engineering Association.

Spaans, M., Spoelstra, M., Douze, E., Pieneman, R., & Grisogono, A. (2009). Learning to be Adaptive. In *Proceedings of the 14th ICCRTS*, Washington, DC, June 15-17. Washington, DC: DoD CCRP.

Woltjer, R., Pinska-Chauvin, E., Laursen, T., & Josefsson, B. (in press). Towards understanding work-as-done in air traffic management safety assessment and design. *Reliability Engineering & System Safety*. doi:10.1016/j.ress.2015.03.010.

Woods, D. D. (2006). Essential characteristics of resilience. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 21–34). Aldershot, UK: Ashgate.

Woods, D. D. (in press). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*. doi:10.1016/j.ress.2015.03.018.

BALANCING GOAL TRADE-OFFS WHEN DEVELOPING RESILIENT SOLUTIONS: A CASE STUDY OF RE-PLANNING IN AIRLINE OPERATIONS CONTROL

Floor Richters 1, Jan Maarten Schraagen1,2 and Hans Heerkens1
1 University of Twente, Faculty of Behavioural, Management and Social Sciences, P.O. box 217, 7500 AE Enschede, the Netherlands
f.richters@utwente.nl, tel. 0031612971613; j.m.c.schraagen@utwente.nl; j.m.g.heerkens@utwente.nl
2 TNO Earth, Life and Social Sciences, Kampweg 5, 3769 DE Soesterberg, the Netherlands
jan_maarten.schraagen@tno.nl

Abstract

The main question this paper aims to shed light on is how goal prioritizing and action planning are distributed across stakeholders over the re-planning process, and what mechanisms can contribute to arriving at integrated and resilient solutions when balancing trade-offs. This will be illustrated by examining a case study on the re-planning process during a safety related contingency event in a single Airline Operations Control Centre. Results show that goal prioritizing authority rotates during the re-planning process across two dominant stakeholders, who shift the dominant trade-off between the boundaries of safety, economics, and operational feasibility. Rotation of authority might have affected awareness of interdependencies between stakeholders, and increased shared situation awareness and maintaining common ground as perspectives broadened. Furthermore, despite time and effort needed to coordinate distributed activities, efficiency was gained by trading-off thoroughness on the least important boundary, and by using loose definitions of common goals. As this helped to balance fundamental trade-offs, tightly controlled operations close to the boundary of acceptable performance were successfully sustained.

1 INTRODUCTION

One of the most fundamental questions in the design of resilient solutions in the face of real world unexpected events, is how to cope with ill-structured and conflicting goals. Goal conflict does not need to be eliminated, instead organizations should be able to balance the various trade-offs across goals (Woods, Dekker, Cook, Johannesen & Sarter, 2010). This balancing act is never ending, as events unfold during the problem solving process and additional aspects of events are revealed and new goals emerge. This requires a continuous re-planning of actions (Klein, 2007). The need to manage conflicting and emergent goals is complicated further by the involvement of multiple stakeholders with different interests and responsibilities, especially when the organisational structure is at least partly based on a network instead of a hierarchy (De Bruijn & Heuvelhof, 2008). This requires additional coordination effort (Hoffman & Woods, 2011). The main question this paper focuses on is how goal prioritizing and action planning are distributed across stakeholders over the re-planning process, and what mechanisms can contribute to arriving at integrated and resilient solutions.

This paper seeks to advance our understanding of the development of resilient solutions across stakeholders who operate in a network. The aim is to look beyond the general control structure that is used to coordinate distributed activities. Rather, its first aim is to identify how goal prioritizing is managed within the process of developing solutions by multiple actors in different parts of an organisation during an unexpected event. Second, we aim to point out the possible consequences of the division of goal trade-off activities on the resilience position of the organisation. This will be illustrated by examining a case study on the re-planning process during a safety related contingency event in a single Airline Operations Control Centre (AOCC).

2 AIRLINE OPERATIONS CONTINGENCY PLANNING IN A NETWORK PERSPECTIVE

The airline under study uses a matrix organisation structure. Authority is divided vertically by functional area and horizontally by cross-functional processes. Consequently, decision making at any time can both have hierarchical and network like characteristics. In an AOCC, network like decision making dynamics seem abundant, especially during large scale disruptions as multiple stakeholders are added to the decision process.

During daily operations in an AOCC, small scale disruptions happen relatively frequently. Disruptions will often lead to delays or cancellations (Thengvall, Bard & Yu, 2000), which can result in excessive delay costs (Wu, 2005). Although they can be complex, the overall impact and duration of this type of events is usually limited, and they are solved within the ongoing operational process. Decision authority is centred in the Operations Control

department, where professionals are constantly challenged to make conflicting trade-offs between the main elements of an airline operation: passenger flows, aircraft and crew (Kohl, Larsen, Larsen, Ross & Tiourine, 2007). As such, their main responsibility is to balance the different interests across the departments that are represented in the AOCC, like crewing and maintenance.

Large scale disruptions on the other hand, can last over longer time periods. Often they extend beyond the boundaries of the AOCC departments. At the airline studied here, under such circumstances decision making is separated from the daily operation. An off-line decision process, led by a Contingency Team, is installed on a case-by-case basis. As additional stakeholders outside of the AOCC are involved as well, this raises the possibility of conflicting interests and makes solving these problems increasingly complex. Moreover, it amplifies the network dynamic of decision making.

Complicating the challenge to balance the interests of multiple stakeholders even further, are the complex interdependencies between the different departments (Abdelghany, Abdelghany & Ekollu, 2008; Clausen, Larsen, Larsen & Rezanova, 2010). Inevitably, this puts a strain on the airline's boundaries of acceptable performance. Over the past years, many airlines have been struggling to meet their economic targets, which can jeopardize safety awareness (Madsen, 2013). As slack between different system components decreases, safety can be compromised due to economic pressure, stimulating the tight coupling of systems to gain efficiency. These developments lead to an increasing risk of large scale accidents, and recovery from such accidents is harder (Cook & Rasmussen, 2005).

The case studied in this paper aims to show how, despite these challenges, several mechanisms could have contributed to sustain resilient performance during the airline's contingency re-planning process. As actions change based on goal prioritization and perception, so does the immediate resilience position of the organisation within its boundaries of acceptable performance (Rasmussen, 1997). Resilience is not just determined by an organisation's current position, but also by its propensity to "go solid" (Cook & Rasmussen, 2005). To gain a richer image of resilient performance, additionally the continuous effort across the re-planning process to balance the five fundamental trade-offs as identified by Hoffman and Woods (2011) is studied: respectively the optimality-resilience trade-off, the efficiency-thoroughness trade-off, the reflection-revelation trade-off, the acute versus chronic goals trade-off, and the concentrated-distributed action trade-off.

3 METHOD

The current study focuses on the re-planning process that was centred around the recovery from an incident in Nigeria, where flight operations temporarily came to a halt due to political unrest and fuel shortages that posed immediate threats to safety. Over the course of two weeks, approximately ten meetings were held, each lasting about an hour. Several different internal and external AOCC departments were involved in the decision making process: Operations Control (both operations personnel and management), Flight (representing cockpit crew), Inflight (representing cabin crew), Maintenance, Security Services, Outstations (representing local operations at the airport in Nigeria), Commercial (representing passenger interests), and Cargo. For the remainder of this paper, Flight and Inflight are subsumed under the heading of Flight, as their interests in this case were the same. The same goes for Commercial and Cargo, who are subsumed under the heading of Commercial. Central to these meetings was the question if and how operations to Nigeria should be sustained.

Analysis is based on data stemming from observations documented by the researcher during the contingency management process, retrospective interviews with all contingency team members, and policy documents, such as the contingency management master plan and official meeting reports. All documents and interview transcripts were coded to identify the actions taken and goals pursued by the different stakeholders. Statements related to the fundamental trade-offs were coded as well. They were linked to the inductively identified driving forces that seem to shape the decision making process.

4 DECISION POINTS

The entire contingency process revolved around three central decision points. First, a decision needed to be made whether or not to evacuate the crew out of Nigeria. When crew was indeed evacuated, the next question was if and how alternative operations should be constructed. Finally, the moment to return to normal operations was decided on. Although official procedures provide clear demarcation between decision points that are embedded in the contingency management process, substantive decision points are subject to discretion of individual stakeholders. This includes, for example, the decision to call off a contingency: *"If circumstances are in agreement with one of the mentioned criteria, [the Duty Manager (DM)] will contact [Operations Control Management] in*

order to start the contingency management procedure. It is impossible to set hard limits for the specific circumstances and it is left to the discretion and professionalism of the DM."

Results are presented for each decision point separately, showing how the decision making process and resilience position evolved over time. In general, throughout the entire process, goal prioritization centred around three main boundaries of performance: safety, operational feasibility, and economics. Operational feasibility includes all necessary flight operations logistics, such as ground handling and maintenance facilities.

4.1 Decision Point 1: Crew Evacuation

Flight operations to destinations in unstable countries are monitored tightly by the airline's Security Services department. Findings are discussed routinely in the Security Committee, in which Security Services and several AOCC stakeholders are represented (including Operations Control and Flight). Most representatives are operations staff, but due to the nature of the case at hand, Flight was also represented by high level executives.

The case studied here centres around local uproar in Nigeria. Although political unrest in this country is not uncommon, tensions were growing alarmingly fast due to local strikes over fuel prices. These strikes created problems for both fuel availability and safety. With Nigeria being a long-haul destination, the flight crew on the outbound journey does not operate the immediate inbound return flight, but overnights in a local hotel. For several days, operations had already come to a halt as crew was kept inside the hotel for safety reasons, since traveling between the crew hotel and the airport was considered to be problematic. Ultimately, the decision was made in the Security Committee to evacuate the crew out of Nigeria entirely. It was not until this moment that Operations Control officially called off a contingency.

Prioritizing goals

Based on their hierarchical position, at this point in the decision process, Flight was the stakeholder in charge of prioritizing goals. Effectively, they decided to trade-off safety over economics. Although officially Security Services does not have decision making authority, they weigh in heavily on this decision by signalling that the score of safety threatens to become unacceptable. Moreover, in expectation of the upcoming decision by Flight, Security Services has already taken into account the economic consequences that giving off this signal might have: *"From a security perspective […] it is easy to say we need to cease operations, but that will cost the airline a lot of money, so we think twice before saying anything like that"*. Security Services also prioritizes safety over operational feasibility: "*Is logistics or safety the main concern? Security Services, whose opinion I value highly, strongly suggested safety*". Hence, goal prioritization was influenced mainly horizontally by one stakeholder, even though authoritative power for the final decision is organised vertically.

Balancing trade-offs

The first difficult trade-off was choosing between different perspectives on the safety status, as these varied widely. Local Security Services contacts signalled that things were taking a turn for the worse, but on the other hand this was contradicted by observations from the airline's local outstations organisation. Moreover, other airlines also seemed to be divided on the subject, as some had halted their operations, but others had not. However, this contrast of perspectives was not considered problematic. Seeking out different perspectives is even encouraged, because it helps to create shared situation awareness: *"Not everybody perceived the same urgency […] but that's a good thing, because otherwise you never have the constructive discussion which is needed to come to the right decisions"*.

Operations in unstable countries always operate closer to the boundary of acceptable performance. This is acceptable, as long as movement is restricted and brittleness is minimized. The actions taken were a direct result of the perceived increase in the brittleness of the system: *"in general the situation was just very unstable and dangerous, aggressive […] you know things can get out of hand any moment."* The negative balance on this optimality-resilience trade-off impacts the balance on the thoroughness-efficiency trade-off. Instead of more thoroughly analysing the situation to get a better grip on the differing perspectives, crew is evacuated when an opportunity comes along to evacuate on a different airline: *"All of a sudden there was an opportunity. […] Another airline who was evacuating its crew offered to take our crew as well."*

Evacuating the crew had a short term decreasing impact on safety (as crew transport was evidently more dangerous than staying inside the hotel), but long term safety and other chronic goals, such as professionalism, were considered to be more important: *"We want to be able to say we have stepped in, and have stepped in in time. Which also enhances long term faith in our company. So it's also a strategic choice."* Summarizing, it seems that based on an unbalance on trade-offs regarding brittleness and a multitude of perspectives, an efficient, opportunistic but conservative approach is taken as chronic goals are considered most important.

Re-planning activities in the Security Committee are clearly distributed. Security Services weighs information, but taking action is a local responsibility. Because of close interdependencies, actions of one department always affect others. Flight, as the dominant decision maker, is aware of this. They balance the distribution of their decision making authority by making additional coordination effort through ensuring decision support by consulting in advance on an operational level with various other AOCC stakeholders about possible alternatives: *"You have to take the perspective of the AOCC organisation into account"*.

4.2 Decision Point 2: Establishing an Alternative Operation

After crew evacuation and calling of a contingency, the second decision point revolved around whether or not to establish an alternative type of operation. Once Flight determined that continuing operations in their current form was no longer an option, authoritative power shifted to Operations Control. Several Contingency Team meetings followed, in which the same AOCC departments were represented as in the Security Council. Additionally, Security Services was added, as were the two Commercial departments. An operational level AOCC planning team was instructed to start searching for alternatives. Very early on in this process, a dominant option surfaced and was selected. It was decided to continue operations, but with a crew slip in a different location. Effectively, this means that a third stop was added to the original flight schedule.

Prioritizing goals

Goal prioritizing authority shifted to higher level management Operations Control. The prevalence of safety did not change, and the option of reinstating normal operations at this point was excluded. Although the addition of Commercial to the decision making process would seem to signal the increasing importance of the economic boundary, operational feasibility was given priority over economics: *"Safety first, then operational feasibility, then economics"*, *"Economics are less important. It is more important to be able to transport everything logistically"*. Moreover, Commercial stakeholders indicated that their main task during the contingency meetings is not to deliver input, but to gain information based on which they can stop or continue to sell flights to customers. Hence, like many of the other AOCC stakeholders, they are treated as a resource department.

Balancing trade-offs

After crew evacuation, direct brittleness of the system was greatly reduced. However, not operating at all over the long term was also seen as brittle, as this would lead to a slow migration of the systems towards the economic boundary. To improve resilience, Operations Control decided to trade-off some of the regained safety in favour of an improved economic position. However, the importance of safety as the number one priority did not change, which was exemplified by the development of a fall back scenario that would have been enacted in case safety would have become problematic during alternative operations. Hence, although the system moved back towards the safety boundary, operations were tightly controlled, decreasing overall brittleness and sustaining resilient performance.

Perspectives on the safety situation still varied. This became especially apparent when Outstations decided to keep expats stationed locally in Nigeria, despite advice of Security Services to move to the compound. This also reflects the distributed authority of stakeholders where their own resources are concerned: *"Everyone knows in his role what to do"*, *"I'm not responsible for fuel. I'm not responsible for the station facilities, […] I want to know that the hotel for my crew is good enough"*. This modularity of activities helps to reduce complexity, and most stakeholders find this combination of differing perspectives and distribution of activity very useful and constructive: *"We respect each other's decisions […] We hold meetings to listen to each other's judgment. To me that's crucial. But of course we can question each other."* Here, the risk of fragmentation due to different perceptions and distribution of activities is likely counterbalanced by maintaining common ground: *"The entire contingency team helps to solve each other's problems."* Moreover, all stakeholders carry out their tasks with one shared purpose in mind: *"keep the operation going"*. Interesting to note however, is that definitions of what this exactly entails varied from acute economic or passenger goals, to chronic strategic goals.

Another way to balance effectiveness of the decision process despite distribution of authority, was limiting the range of options that were considered. Although several options were available, such as other crew slip locations or even rebooking passengers on flights of other airlines, these were not considered. *"From a pragmatic perspective you immediately search for a solution to start operations as soon as possible"*, *"We have jumped on the first opportunity to restart operations with an alternate crew slip"*. This satisficing behaviour was largely based on past operations and on actions of partner airlines. Although it is highly efficient, corners were cut on thoroughness. Moreover, it mostly discounts the economic perspective: *"It is not about economics* […] *it is really all about recovery speed."* This seems to emphasize that acute economic goals are not seen as very important. The lack of thoroughness, mainly at the cost of economics, seemed acceptable based on the short term focus of the

solution: *"This solution will work for days, not weeks"*, *"First let's make sure we offer an alternative. Phase two is focusing on what we actually want."*

4.3 DP 3: Return to Normal Operation

After start-up of the alternative operation, the Contingency Team's main task was monitoring that operation. At the same time, the Planning Team was asked to continue to look for other options, because the current alternative would not be not sustainable in the long run. However, after a few days local circumstances in Nigeria changed, and the decision was taken to return operations back to the original schedule.

Prioritizing goals

The decision to reverse the alternative operations was enabled by the positive judgment of safety by Security Services, in consultation with Flight. Again, safety is given the highest priority. Although the original decision to halt operations was made solely by Flight, the final decision to reverse operations was made together with Operations Control, as they have final authority over operational feasibility.

Balancing trade-offs

The risk of brittleness was minimized by the continued close monitoring of the security status and the running alternative operation. Once Security Services reported that safety started to improve, operations were not directly reinstated. Flights were scheduled up to three days ahead, creating slack that allowed the Contingency Team to await if stability would persist. This also allowed for integration of all the different perspectives within the team, as other airlines started operating again as well, and outstation reports were okay.

Although efficiency seemed to be favoured during setting up the alternative operation, thoroughness prevailed here: *"Triple check if there is fuel available, because I want to make sure we can leave there."* Still, many stakeholders felt that the return to normal operations did not take too long and was relatively efficient. Moreover, it again shows an opportunistic but conservative approach and a focus on chronic safety goals.

5 DISCUSSION

This paper attempts to show what mechanisms seem to play a role in maintaining resilient performance in a network environment where responsibilities and activities are distributed across multiple stakeholders during re-planning of operations. Despite the involvement of higher level executives for Flight and Operations Control, the rotation of decision making authority gives the decision making process a network dynamic. During the search for an alternative operational mode, each of the resource departments maintains its authority to block the decision making process. This exemplifies the horizontal distribution of autonomy over resources.

The distribution of activities across stakeholders likely has contributed to the multitude of perspectives that existed over the first two decision points. Diversity of perspectives is important to ensure timely identification of safety issues (Hayes, 2012). Moreover, discussing these perspectives helped to create shared situation awareness and common ground, helping to improve resilient performance (Gomes, Borges, Huber & Carvalho, 2014; Vidal, 2009). However, coordination of activities and integration of perspectives requires considerable time and effort, which are usually in short supply in AOCC environments (Igbo, Higgins, Dunstall & Bruce, 2013).

Several dynamics could have balanced this issue. First, efficiency was sometimes traded off in favour of thoroughness, but only where the least important, economic goal was concerned. Although decision making authority rotates, goal priorities throughout the development of this case are fixed: safety comes first, operational feasibility second, and economics third. The dominant trade-off does shift over time as the system moves back and forth between boundaries, but as safety is always given highest priority, marginal boundaries are relatively fixed. Moreover, operating close to this boundary is only acceptable when the position can be tightly controlled, which is typical for a high reliability organization (Cook & Rasmussen, 2005). The marginal boundary on operational feasibility on the other hand, is more flexible. Most flexible and least important, at least for a contingency during a relatively short time frame, is the economic boundary. Compromising thoroughness mostly on this boundary helped to maintain focus on chronic goals.

Second, maintaining common ground was based on a very vaguely defined common goal, in this case 'continuing some form of operation'. Using a loose definition could have helped to sustain resilient performance, as such 'constructive ambiguity' offers stakeholders room for adjusting actions to their own objectives (De Bruijn & Heuvelhof, 2008). Using a loose definition also prevents having to take into account a large number of decision making variables, which reduces complexity (Kontogiannis & Malakis, 2013).

6 CONCLUSION

The main question this paper focused on is how goal prioritizing and action planning are distributed across stakeholders over the re-planning process, and what mechanisms can contribute to arriving at integrated and resilient solutions. Results have shown that goal prioritizing authority rotates during the re-planning process across two dominant actors. Rotation of authority might have affected awareness of interdependencies between stakeholders, and increased shared situation awareness and maintaining common ground as perspectives broadened. Furthermore, despite time and effort needed to coordinate distributed activities, efficiency was gained by trading-off thoroughness on the least important boundary, and by using loose definitions of common goals.

REFERENCES

Abdelghany, K. F., Abdelghany, A. F., & Ekollu, G. (2008). An integrated decision support tool for airlines schedule recovery during irregular operations. *European Journal of Operations Research*, *185*(2), 825-848.

Clausen, J., Larsen, A., Larsen, J., & Rezanova, N. J. (2010). Disruption management in the airline industry – Concepts, models and methods. *Computers & Operations Research*, *37*(5), 809-821.

Cook, R., & Rasmussen, J. (2005). "Going solid": a model of system dynamics and consequences for patient safety. *Quality and Safety in Health Care*, *14*(2), 130-134.

De Bruijn, J. A., & Heuvelhof, E. F. (2008). *Management in Networks: On multi-actor decision making*. Abingdon: Routledge.

Gomes, J. O., Borges, M. R., Huber, G. J., & Carvalho, P. V. R. (2014). Analysis of the resilience of team performance during a nuclear emergency response exercise. *Applied ergonomics*, *45*(3), 780-788.

Hayes, J. (2012). Operator competence and capacity–lessons from the Montara blowout. *Safety science*, *50*(3), 563-574.

Hoffman, R. R., & Woods, D. D. (2011). Beyond Simon's Slice : Five Fundamental Trade-Offs that Bound the Performance of Macrocognitive Work Systems. *Intelligent Systems, IEEE, 26*(6), 67-71.

Igbo, K. E., Higgins, P. G., Dunstall, S., & Bruce, P. J. (2013) Regulating Interactions across Multiple Centres of Control: An Airline Operations Control Perspective. In I. Herrera, J.M.C. Schraagen, J. van der Vorm, & D.D. Woods (Eds.), *Proceedings of the 5th International Resilience Engineering Symposium: Managing Trade-Offs* (pp. 29 - 36). Sophia Antipolis: Resilience Engineering Association.

Klein, G. (2007). Flexecution as a paradigm for replanning, part 1. *Intelligent Systems, IEEE*, *22*(5), 79-83.

Kohl, N., Larsen, A., Larsen, J., Ross, A., & Tiourine, S. (2007). Airline disruption management – Perspectives, experiences and outlook. *Journal of Air Transport Management*, *13*(3), 149-162.

Kontogiannis, T., & Malakis, S. (2013). Strategies in coping with complexity: Development of a behavioural marker system for air traffic controllers. *Safety science*, *57*, 27-34.

Madsen, P. M. (2013). Perils and Profits: A Re-examination of the Link between Profitability and Safety in US Aviation. *Journal of Management*, *39*(3), 763-791.

Rasmussen, J. (1997). Risk management in a dynamic society : a modelling problem. *Safety science*, *27*(2), 183-213.

Thengvall, B., Bard, J., & Yu, G. (2000). Balancing user preferences for aircraft schedule recovery during irregular operations. *IIe Transactions*, *32*(3), 181-193.

Vidal, M. C., Carvalho, P. V., Santos, M. S., & dos Santos, I. J. (2009). Collective work and resilience of complex systems. *Journal of Loss Prevention in the Process Industries*, *22*(4), 516-527.

Woods, D. D., Dekker, S., Cook, R. I., Johannesen, L. J., & Sarter, N. B. (2010). *Behind human error* (2nd ed.). Farnham: Ashgate.

Wu, C. L. (2005). Inherent delays and operational reliability of airline schedules. *Journal of Air Transport Management*, *11*(4), 273-282.

MANAGING CLIMATE RESILIENCE FOR THE EUROPEAN AVIATION SECTOR: PROACTIVELY ADAPTING TO A CHANGING WORLD

Rachel BURBIDGE [1]
[1] EUROCONTROL, Rue de la Fusée 96, Brussels, B-1130, Belgium
[1] rachel.burbidge@eurocontrol.int, +32 2 729 3451

Abstract

The forecast impacts of climate change, such as sea level rise, higher temperatures and greater weather extremes pose an operational and business risk for European aviation (EUROCONTROL, 2013; Thomas et al., 2009). In order to mitigate this risk it is essential for the sector to develop increased resilience to those hazards at both organisational and network level. This will be achieved by: reducing vulnerability to and increasing the capacity to recover from perturbation; and, proactively adapting operational and business practices to manage the impacts of a changing climate (Folke et al., 2010).

In order to achieve this efficiently and cost-effectively, it is essential for the sector to act proactively. In consultation with stakeholders, EUROCONTROL has developed five key recommendations to promote cost-effective climate resilience within the sector. These include local and network-wide risk assessment, better use of MET information and the implementation of 'no-regrets' or 'win-win' measures which also address issues such as capacity. A growing but limited number of stakeholders are already implementing comprehensive resilience measures. Yet, a survey of European aviation organisations shows that although awareness is growing many stakeholders are still not acting, often due to a lack of information and guidance. It is therefore essential to identify and address the barriers which are currently preventing action. Overall, climate change is an issue of risk management and early action is the key to cost-effective mitigation of those risks (EUROCONTROL, 2013).

The autghor presented the following subtopics:

- What are the key climate change impacts which the aviation sector can expect to face and what are the operational and business risks from those impacts? What are the timescales in which we can expect to experience them and how will they vary across the sector (e.g which impacts will affect en- route traffic and which will affect airports)?
- What can the sector do to develop resilience to those risks at both individual organisation and network level?
- Why is it necessary to address resilience at multiple scales (Folke et al., 2010)?
- What are the barriers which are currently preventing action within the sector and how can they be addressed (Moser and Ekstrom, 2010; Burbidge, 2014)? How can we develop a culture of resilience thinking within the sector?
- Why is it crucial to take proactive action rather than waiting for impacts to become more severe (EUROCONTROL, 2013)?
- How can we measure the effectiveness of the resilience measures which are implemented? Firstly, we need to quantify the base level of network resilience and the corresponding impact of a disruptive event in order to facilitate the development of mitigation actions. Generic resilience metrics are currently being developed by a number of organisations. How do these apply to climate change resilience and are there specific metrics which are required?
- Could a resilience key performance indicator (KPI) facilitate more proactive reactions to disruptive weather by identifying an event-specific performance goal which is aligned with ATM capacity management and flight safety requirements?

The actions which the air transport sector needs to take to develop and manage resilience to the impacts of climate change. It will examine a range of measures including generic measures such as softer actions (training, best practices) and no-regrets or win-win actions. As many of these are applicable to both the wider transport sector and other key sectors as this contributes to developing cross- sectoral knowledge on developing and managing resilience. It will also emphasise the importance of building resilience at organisational level so as

to contribute to developing larger scale system resilience and reduce overall system vulnerability (Folke et al., 2010, EUROCONTROL, 2013).

A key part of managing resilience is measuring the effectiveness of resilience measures so that they can be reinforced or redesigned if they are underperforming, not fit for purpose or the risk profile changes. Therefore the paper will highlight the need to develop appropriate metrics and performance indicators to achieve this. Finally the paper will emphasise the need to take proactive action so as to increase cost-effectiveness and reduce damages and risk. It will focus on how to break down barriers to adaptation so as to raise awareness and motivate proactive action.

REFERENCES

Burbidge, R. (2014)Aviation Climate Resilience: Clarifying the Impacts and Identifying the Barriers, 18th Air Transport Research Society (ATRS) World Conference, Bordeaux, 17-20 July 2014

EUROCONTROL (2013) *Climate Change Risk and Resilience,* Challenges of Growth 2013, EUROCONTROL, Brussels

Folke, C., S. R. Carpenter, B. Walker, M. Scheffer, T. Chapin, and J. Rockström. 2010. Resilience thinking: integrating resilience, adaptability and transformability. Ecology and Society 15(4): 20. [online] URL: http://www.ecologyandsociety.org/vol15/iss4/art20/

Moser, S. C. and Ekstrom, J. A. (2010) *A framework to diagnose barriers to climate change adaptation*, Proceedings of the National Academy of sciences, Vol. 107 (51) p.22023-22031 [online] http://www.pnas.org/content/107/51/22026.full

Thomas, C., McCarthy, R., Lewis, K., Boucher, O., Hayward, J., Owen, B., and Liggins, F (2009) *Challenges to Growth Environmental Update Study*, EUROCONTROL, Brussels

RESILIENCE ENGINEERING (RE) IN DESIGN: INITIAL APPLICATION OF A NEW RE ASSESSMENT METHOD TO THE MULTIPLE REMOTE TOWER CONCEPT

Ivonne Herrera[1], Anthony Smoker[2], Ella Pinska-Chauvin[3], Beatrice Feuerberg[4], Michaela Schwarz[5], Tom Laursen[2], Billy Josefsson[6]
1 SINTEF, Norway, Ivonne.A.Herrera@sintef.no
2 IFATCA & Lund University, Anthony_John.Smoker@lucram.lu.se
2 IFATCA & NAVIAIR, Denmark, mettom@private.dk
3 EUROCONTROL, France, ella.pinska-chauvin@eurocontrol.int
4 NORACON/ (On behalf of AVINOR), France Beatrice.feuerberg@egis.fr
5 NORACON/ Austro Control GmbH, Austria, michaela.schwarz@austrocontrol.at
6 NORACON/LFV, Sweden, billy.josefsson@lfv.se

Abstract

The paper presents initial application and further development of a resilience engineering (RE) assessment method to the multiple remote towers (MRTWR) concept. The RE method is operationalised through a set of eight principles identified from existing RE literature. These principles are 1) Work-as-Done; 2) Varying conditions; 3) Signals and Cues; 4) Goal trade-offs; 5) Margins and adaptive capacity; 6) Coupling, interactions and cascades; 7) Timing, synchronisation and time scales; and 8) Under-specification and approximate adjustments. The application of the RE method to the concept of MRTWR has helped to understand the significance of the change and associate design requirements at a larger scale, focusing not only on the function of specific components, but on the ATM system as a whole. Results from this application show how understanding everyday operations (work-as-done) helps to evaluate the gaps between current and envisaged design of a new operational concept (MRTWR). Based on work-as-done the principles are used to develop design requirements how to enhance resilient performance of systems. Sharing this experience may offer practitioners and researchers from aviation and other domains the opportunity to build on lessons learnt from this application to investigate how resilience can be enhanced in their systems.

1 INTRODUCTION

Resilience Engineering (RE) is 'the scientific discipline that focuses on developing the principles and practices that are necessary to enable systems to function in a resilient manner' (Hollnagel, 2014). According to Hollnagel (2011) resilience is defined as the ability of a system to adjust to changing conditions (expected or unexpected) in order to sustain required operations. As such RE requires a mind set change moving from classic safety assessment approaches towards approaches addressing the dynamics of complex socio-technical systems in context. The body of RE knowledge and practices is under continuous development and evolution. Methods and approaches to describe, assess and measure resilient system performance have evolved over the past decade, but still need further development and practical validation.

2 RESEARCH GOALS, METHOD AND DESIGN

2.1 Research goal

The research goals of this activity were firstly, to demonstrate added value of the RE assessment method to the MRTWR concept in the design phase with respect to classical safety approaches (complementing work-as-imagined with work-as-done). Secondly, to refine and further develop the RE assessment method in terms of improving its guidance for application to a wider community of practitioners based on practical lessons learnt.

About the new MRTWRS concept: Provision of Air Traffic Services (ATS) is costly and there is a need to increase cost-efficiency, particularly at low to medium density airports. A possible way to reduce costs without reducing the level of safety is the Remote Tower concept in which the provision of ATS is no longer located at the aerodrome and will be re-located to Remote Tower facility. In Multiple Remote Tower operations, ATS may be provided simultaneously to more than one aerodrome by a single controller from a remote location.

Air Traffic Management is undergoing a significant shift in its evolution as a part of the European Commission Single European Sky strategy. Single European Sky Air Traffic Management Research (SESAR) is the research and

development foundation for the eventual implementation. The RE method was developed to augment the current Safety Reference Material for safety assessments of new operational concepts in SESAR. In addition possibilities and capabilities of RE beyond SRM will be explored. Thus application of the RE Method is for the assessment of resilience in new concepts/designs for implementation in ATM.

The SESAR programme includes safety within its compass. The SESAR work includes the development of Safety Reference Material (SRM) that can be applied to safety assessment of SESAR projects. The SRM includes a section addressing deployment and the development of guidelines for the safety assessment of resilience in new ATM designs (called hereafter RE Guidelines). Subsequent SESAR projects have been instigated that further develop RE Guidelines and associated methodology exploring resilience engineering in new design of systems in the design phase of an operational concept.

The RE Guidelines are a structured approach to the application of the RE method. This is an iterative exercise that requires a multidisciplinary team composed of designers, practitioners and researchers. The nature of the changes within the social-technical system – which the ATM system is representative of – are varied. These changes typically involve changes to procedures, the introduction of new technology and changes in tasks – the work undertaken – by the human. The extent of these changes, increasingly involves the interaction between organizations, increase use of new technologies, airport actors, pilots and controllers at the operational interface. Experience of earlier implementations of the RE guidelines has found that new system behaviours emerge from new interactions and dependencies that were not previously identified in safety assurance activities. Emergent properties are defined by Woods as a system property, arising in the interactions across components, subsystems, software, organizations, and human behaviour (Woods, 2006). Safety is in and of itself an emergent system property.

Safety in ATM is currently assessed and measured using classic safety assessment techniques that are well defined in ESARR 4 & 5 [Eurocontrol, 2001; Eurocontrol, 2002]. It has been recognised that these classical approaches have limitations [Sheridan, 2007, Hollnagel, 2013], particularly the gap between safety assessment of systems in the design and pre-implementation phase and the subsequent operational implementation. This is particularly pertinent with regard to the nature of the functional work of the system – the control and management of air traffic. Frequently this is investigated in terms of work-as-imagined (WAI), and not as work-as-done (WAD) (Hollnagel, 2014).

The issue is further exacerbated, in that the work to be undertaken – the future work-as-done itself - is changing, just as work-as-done currently it naturally changes too. The limitations of the capability of simulation facilities (i.e. an ATC simulator can never replicate the real environment including all relevant interfaces, features, processes and procedures) and the approach to system development means that safety assessment of new designs is perforce limited and the real nature of work-as-done is therefore underspecified. The nature of simulation facilities in ATM is such that it is rare to replicate the varying conditions that are experienced in the operational environment. Additionally, the multiplicity of interaction with other actors and agencies is wide and is impracticable to simulate fully. The concept of operations itself is often underspecified. These varying conditions significantly influence system behaviour, and thus leave work-as-done underspecified as well. The application of the RE assessment method MRTWRS explores resilience engineering to address these issues.

2.2 Resilience Engineering Guidance

This iteration of the application of the SESAR resilience engineering guidelines built on those delivered in 2014 A first application of the guidelines was developed to the concept Initial Four Dimension Trajectory/ Controlled Time of Arrival (i4D/CTA) representing a technological and operational change to improve operations in 2012. This application identified additional safety and design requirements that traditional safety assurance processes did not identify (Woltjer et al. 2013, Woltjer et al, 2015).

The experience of the initial application of the RE method to the i4D concept provided the impetus to explore the concept further and apply the RE guidelines elsewhere within the SESAR ATM activities. One major need that emerged related to the practical application and operationalisation of RE to improve the RE assessment. The expected benefits were to make the guidance more practical and easily applicable for safety practitioners. Applying the guidelines should not require acquisition of in-depth scientific knowledge or expertise. Additionally, the need for a methodology *per se* was identified.

The intent was to further develop the RE guidelines and refine a methodology in a way that it can be applied to a range of different Air Traffic Management system changes and to extend the existing SESAR SRM method. An additional goal was to develop an accompanying RE familiarisation and training package for practitioners based on easy-to-understand and practical real-life examples (how to cook an egg, how to enter a roundabout when

driving) but also ATM examples. The training package delivers the new RE language, terms and definition as well as system thinking.

Resilience Engineering Principles in SESAR

RE is operationalised in the guidelines through eight principles. The eight principles are shown in figure 1, with an exemplar of each principle added. Each principle represents a *lens* by which to explore the system characteristics, properties and the nature of work-as-done in the current operation and in the new design in terms of specific RE attributes. With the knowledge thus gained it is possible to explore the hypothesised work, as will-be-done using the same lens to explore the resilience of the new design.

The focus of the exploration is day-to-day work (Work as Done) what external (non-operational) observers see as adaptations needed to get the work done. Variations (internal or external), trade-offs and goal conflicts, are seen and perceived by those performing the work as normal. The eight RE principles therefore provide the means by which to carry out the operational exploration of work-as-done and principles were drawn from RE theory. This is the basis for exploring resilient performance, the analytical frame with which to explore resilience and, is entirely consistent with the projects working definition of resilience engineering (Hollnagel, 2014).

The RE guidelines include guidance with which to explore each principle. These form one dimension of an analytical framework with which to frame the exploration of each one of the eight principles. The other dimension is an operational dimension in terms of the services that the work-as-done is serving to fulfil and enact.

Figure 1. Example of principles related to the following operational story: Spacing between two aircrafts at the same level and crossing each other with estimated 3 miles. The example describes Work-as-done and the other seven principles seen through an operators (in this case an Air Traffic Controller) lens. Different scenarios have been used to stimulate the thoughts of the operator to achieve the description.

SESAR Resilience Engineering Assessment Process Phases

An overarching principle of the guidance and methodology is the need for a method that can be generalised to different concepts. The initial process for the application of Resilience Guidance consisted of eight steps. These steps comprised exploring, sequentially, each RE principle with each of the ATM services identified as salient or germane. The guidance material provides exemplars of RE characteristics and operational ATM functions with which to guide the application of the guidance. The RE guidance proposes a number of ways to capture the data, a workshop composed of operational personnel with knowledge and experience of both the current and new designs as well a project team members is the preferred method

Defining each step of the guidance was a key part of assessing the RE Guidelines. A need to improve guidance to personnel involved in the RE principles assessment was addressed through consolidation and simplification of the initial process as described below. The process is in three easy to follow phases a preparation phase, a data

collection phase (workshop) and a data analysis and results phase as illustrated in figure below. Thus, a structured approach to the application of the RE guidance and methodology was developed and tested.

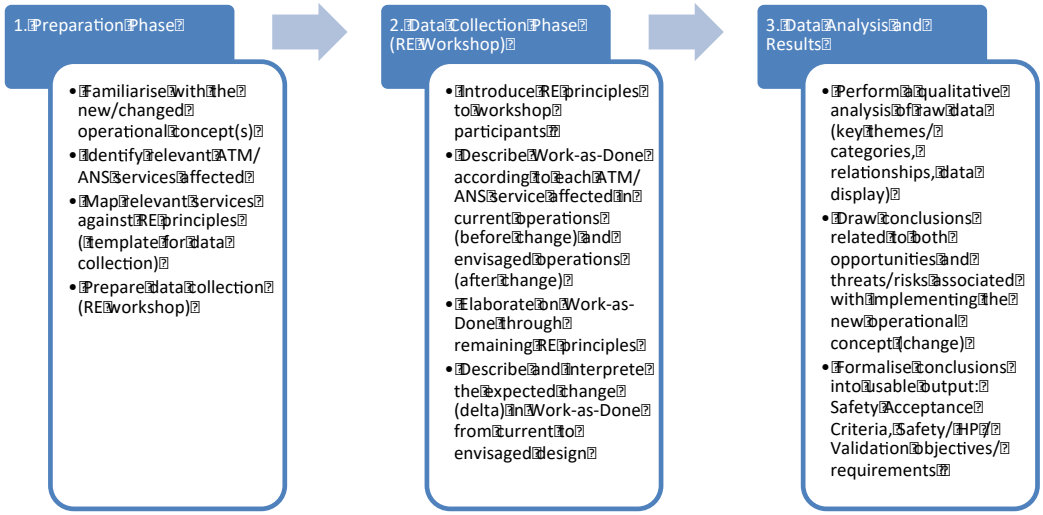


Figure 2. The SESAR RE process phases

1. *Preparation Phase*The preparation phase entails developing an understanding of the new operational concept. The objective of this is preparation for attaining the entry criteria for phase two.
   The preparation phase involves familiarization with the new concept (new design). Typically this will involve a review of the operational concept and design documents and method of operations and procedures. Informal interviews and observation of operations during simulation of live trial activity are also useful for gaining an appreciation operations currently and as envisaged.
   The phase also involves identifying the ATM services in the current and new designs and assessing the salience for inclusion in the workshop. A service represents elements of the purposeful; activity of the system e.g. Sequence aircraft inbound from fix *v* for arrival at runway *n* at airfield *y*; traffic planning and sequencing at airfield z; managing the manoeuvring area at airfield *z*.
   The creation of the ATM Service/RE Principle matrix that will be used to structure the RE Phase 2 workshops and fulfils the entry criteria into phase 2. Along with the organisation and planning of the phase 2 workshop.
2. *2. Data collection Phase (RE workshop)*
   The data collection phase is performed through two days workshop with participation of technical and operational experts together with RE assessment team. During the workshop current and envisioned work is systematically mapped to the most relevant services and principles.
   This phase then is the primary means of data capture in the application of the method. The workshop commences with an introduction to the concept of RE and preparation for the exploration of the ATM services, work as done and the other RE principles.
   Data is captured in a spread sheet and documents the discussion as each principle is discussed in the context of each salient ATM service of the ATM Service/RE Principle matrix. For each principle a description of current operations (Work as Done), description of change in operation (work as envisioned) and delta of the change are captured.
3. Data analysis and results
   The analysis task is essentially one of qualitative analysis of the data obtained from the workshop. Coding of the data can be conducted by identifying pertinent themes and narratives formed by correlating and interpreting participant comments in the context of the themes. From this arguments can be made to support and reason specific conclusions related to design.
   A multidisciplinary team (ATCOs, pilots, safety analysts etc.) performs a qualitative analysis. An initial list of questions related to each principle is provided in the initial guidelines and provides an analytical framework. Results can be used to provide new validation objectives, HMI design, structural and procedural changes of new system designs. The RE Method can also provide insight into the other SESAR Key Performance Areas (KPAs) other than safety e.g. capacity, flexibility, predictability, efficiency,

cost effectiveness, and environment. The conclusions derived provide the basis for recommendations that constitute the results. The use of the workshop narrative can provide a rich picture with which to amplify and emphasise the conclusions.
This process assumes that the analyst team involved in the exercise are familiar with Resilience Engineering and Complex Socio-Technical Systems.
With a light on improving the existing RE method as described above two RE principles were investigated. The first exercise focused on P2 (varying conditions) and a second exercise focused on P4 (goal trade-offs) related to Safety Acceptance Criteria (SAC). SAC are explicit and verifiable criteria that set the acceptable safety level of the implemented change. SAC include not just specific risk targets but also safety (and other), regulatory requirements, operational and equipment standards and practices.

a. The first exercise intends to explore conditions affecting performance variability as a way to understand how and why adjustments are performed. It explores which conditions need to be managed and which adjustments are required. Innovation games create a space where conditions can be identified. The idea is to identify conditions relevant to everyday operations of the Air Traffic Controllers projected to the Multiple Remote Towers concept. An innovation game the Blind Side is selected as game for brainstorming. This game is adapted from Game-storming (Gray, D. et al., 2010), already proven guidelines and templates were used. At the end of the exercise a list of conditions affecting variability for multiple remote towers were gathered. Additionally, way this variability is management and any possible adjustments were identified.
b. The second exercise addresses a key question how can findings from everyday work support updating a risk picture. It aims to understand which Key Performance Areas (KPAs)s are traded-off in specific situations, understand if and how safety may be impacted and understand the contributing factors and multiple effects affecting safety acceptance criteria. After a short introduction on Safety Acceptance Criteria and the process, participants were introduced to the purpose and the logic of the exercise discussing the above questions through specific scenarios related to the new concept. The impact of trade-off in everyday operations within tested scenario was reflected on how it could affect the performance levels such as effectiveness, capacity or cost benefits.

3 RESULTS

The RE guidelines supported assessment of the MRTWR concept by looking into the relevant air traffic services and the eight RE principles using the structure outlined in table 1. Services such as Traffic planning and sequencing, the Navigation function of controller, Meteorological services, Communication (Information / Decision Services), Potential conflict / collision detection and Start-up are the services for which RE provides additional insights.

Aggregated results were summarized through the RE principles in current and envisioned operations and an assessment of the change. Results from the application of the RE guidelines are integrated into the SESAR Safety Assessment Report consequently the assessment output gathered the recommendations in terms of Key Performance Areas such as Human Performance and Safety issues, as well as validation needs.

Table1: Example first two columns show information collected during workshop, last two columns show results from the RE analysis

Service 1: Traffic planning and sequencing	
Current Work-as-done (P1)	In a small airport the traffic patterns and variations are well known. Planning and sequencing of aircraft is seldom an issue. Controllers perform a number of tasks beyond those strictly associated with being a tower controller
Envisioned Work-as-done (P1)	It is uncertain if the MRTWR controller is allowed to operate simultaneous arrivals/departures at different aerodromes. Scanning patterns are extended to incorporate all of the airfields that the MRTWR ATCO is responsible for. PTZ augments and supports scanning patterns.
Assessment of Change Work-as-done (P1)	*D14 Work-as-Done Guide: Which techniques are envisioned to be used with the change to meet changing demands and cope with complexity of everyday situations?* MRTWR controller has a new interfaces human and technical for multiple locations. Nature of MRTWR controller is different because of managing concurrent airfield

Service 1: Traffic planning and sequencing	
	operations. The service should be the same but will at times require prioritization between airfield operations. Local knowledge and multiple remote operations: It is uncertain how local and tacit knowledge is available for other sources
Assessment output (design RE recommendations)	Validation needs: Define interfaces and validate the relationship of the MRTWR controllerand other local actors. How do actors support each other to deliver effective and timely services. Modified scanning patterns pose the risk of selective information search and the controller only activating selected information in the other airfield (e.g. only check one rwy) without actually activating the latest contextual information of the environment. Work is redistributed and the MTTWR controller needs to have sufficient local knowledge to provide effective ATS to aircraft operators and other users of the airfield. Controllers need to be trained and prepare in managing their workload including prioritization of tasks and tasks scheduling for concurrent airfield operations.

Key Findings (Application)

The application of the RE principles to the concept of MRTWRS has helped to understand the significance of systems change at a larger scale, focusing not only on the function of specific components. Hence, as a result, to identify design improvements for the proposed MRTWRS design.

SESAR KPA Safety: evidence of new interfaces and interdependencies

The MRTWRS concept changes the role of the ATCO from being solely dedicated to TWR functions that embraces aerodrome and approach control as well as supervisory tasks in a single person operation to a aerodrome controller providing ATS at two or more aerodromes. The RE workshop tested a number of assumptions and dependencies. Additionally, dependencies between the MRTWR controller, the supervisor (SUP) and remote tower centre (RTC) approach (APP) were explore and the method provided added value in our understanding on how these roles interact. The nature of work for a MRTWR ATCO is different because of managing of concurrent airfield operations. This will manifest in practical terms for traffic planning and sequencing as well as trade-offs when prioritizations have to be made that allow the ATCO to concentrate on specific tasks at a particular airfield. In cases where the MRTWR ATCO has to give priority to one aerodrome (i.e. due to an emergency), it was assumed by workshop participants that a supervisory function was available to coordinate emergency response units and organises management of traffic at the other aerodrome (close airspace or find a second ATCO to take care of aerodrome 2). Another assumption was made regarding the 24/7 availability of an RTC APP unit that will assist the MRTWR ATCO in traffic sequencing. As a consequence, a recommendation was made from the application of the RE method reading: “MRTWR controller, SUP and RTC APP by design provide a cohesive and consistent ATS”. This recommendation goes along with a validation need related to the definition of the interface between MRTWR controller, SUP and RTC approach function as well as their relationship.

SESAR KPA Human Performance : different Scanning Patterns and Workload Prioritisation

The MRTWR controller has a new interface that is currently performed by single TWR controller. RTWR controller prioritization is different for multiple airports e.g. simultaneous take-off operation, two or more aircraft issue take off clearance at same time or two aircraft given landing clearance at same time. In order to accommodate the changing nature of work training need to be provided to support development scanning patterns with the new tools (e.g. runway sweep function, pan-tilt-zoom camera), techniques and new roles. Modified scanning patterns pose the risk of selective information search and the ATCO only activating selected information in the other airfield (e.g. only check the runway) without actually activating the latest contextual information of the environment (e.g. weather). ATCOs need to be trained and prepare in managing their workload including prioritization of tasks and tasks scheduling for concurrent airfield operations.

Key Findings (Development of Methodology)

For the methodology, a more structured documentation (easy-to-use templates), new innovative and creative knowledge elicitation approaches including innovation games and a way to perform analysis (e.g. system thinking, mapping of interdependencies) based on resilience engineering have been proposed. Using a workshop as the principal means of exploring the resilience of the new design can be an effective tool but shouldn’t be the only

one. A toolbox should be provided that gives an overview of suitable RE tools and when they should be used and shouldn't be used. Additionally the important issue of how the design and operational communities – air traffic controllers, engineers, project managers etc. are able to operationalize the RE output has been identified as an important issue to address. As is the nature and substance of the RE output – especially the added value provide to the design and project teams.

Key areas of improvement for the methodology included the fact that RE language (e.g. adaptive capacity, cascading, emergent factors, under-specification, tight coupling etc.) is not easy for practitioners to comprehend, because these terms are not part of their natural language. Project managers and teams need to be prepared and trained to enable an effective interpretation of the results. As a consequence different levels of training are required for different actors (e.g. safety and operational experts, workshop facilitators, data analysts). In this application not all of the system of interest was represented (i.e. the supervisor). It is necessary to represent in the scaled world of the method the key interaction components and entities to create al picture of the ATM system in context as rich as possible. Finally more work needs to be done on the data analysis and objectivity of results. So far it is essentially deductive reasoning, which requires rigour to deliver consistency – but in turn does not produce easily generalizable or repeatable results. Project teams are seeking a high level comparative resilience performance between designs.

In this application the game-storming exercise showed to be an effective approach to capture conditions affecting everyday operations related to a new operational concept (i.e. MRTWR). The SAC exercise identified elements that could potentially influence the SAC and other KPAs via trade-offs. However, the granularity of results showed that collected outputs are arguments for evidence of safety, or about the need to demonstrate with evidence the need for safety, rather than driving the SAC setting process itself. This exercise was focused on investigating goal trade-offs further have potential to provide deeper insights in the affected KPAs and in this application helped to identify which elements are required for possible safety improvements.

4 CONCLUSIONS AND FURTHER WORK

Our argument is that the resilience principles proposed, and deployed in the methodology enhances the understanding of everyday operations. The focus in the guidelines is on understanding everyday operations and exploring the principles (work as done, coupling and cascades, etc.) in anticipation of the future ATM system and to explicit the subtle changes actually brought by the envisioned ATM system. The key is to relate future concept design to work-as-done and to learn from the way in which ATM system (organizations, technical systems and humans) adjust all the time to varying conditions. Learning from work as done, the strategies operators apply to solve complex situations, organization of work, use of new tools deserves to be considered from a systems perspective already in the design phase of an ATM system with the purpose to improve resilient performance. Sharing this experience may offer practitioners and researchers from aviation and other domains the opportunity to build on lessons learnt from this application to investigate how resilience can be enhanced in their systems.

For the methodology, areas of improvement concern a more structured documentation providing practical hands-on guidance when and how to explore resilience in action suitable for practitioners with different backgrounds. The importance of work as done and adaptation within ATM actors as a web of interdependent actors, leads the method to consider further developments addressing sustained adaptive capacity as proposed by Woods (2015).

The methodology should suggest a toolbox of techniques such as innovation games and a way to perform analysis based on resilience engineering have been proposed. Additionally the important issue of how the design and operational communities – air traffic controllers, engineers, project managers etc. are able to make use of the RE output in project activities has been identified as an important issue to address. As is the nature and substance of the RE output – especially the added value provide to the design and project teams. The analysis of the various feedback on the RE methodology and the RE workshop itself leads the project to derive the lessons learned from this application case. Specific areas of improvement have been identified such further developments on operationalization of sustained adaptive capacity. This will be explored further to improve the methodology in general and to provide more detail guidance in its application.

Ackowledgements - disclaimer

The authors would like to thank the organisations and participants who supported this test application. This research is funded as part of the SESAR Joint Undertaking 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.

REFERENCES

Eurocontrol, (2001). ESAAR 4: Risk assessment and mitigation in ATM. Brussels Safety Regulation Commission, Eurocontrol

Eurocontrol. (2001). ESAAR 5: ATS Service Personnel. Brussels, Safety Regulation Commission, Eurocontrol

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

Hollnagel. (2014). From Safety I to Safety II. Farnham, U.K. Ashgate

Hollnagel, E. (2013). A tale of two safeties. International Journal of nuclear safety and simulation. Vol 4; (1)

Hollnagel E., Woods D. D, Leveson, N. 2006. Resilience engineering: concepts and precepts. Ashgate.

Hollnagel, E. (2011). Epilogue: 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.

Hollnagel, E. (2009). The ETTO Principle: Efficiency-Thoroughness Trade-off, Why Things That Go Right Sometimes Go Wrong,. UK: Ashgate.

Sheridan, T.B. (2007). Risk, Human Error, and System Resilience: Fundamental Ideas. Human Factors; Vol. 50, (93) p. 418-426.

Woltjer, R., Pinska-Chauvin, E., Laursen, T., & Josefsson, B. (2013). Resilience Engineering in Air Traffic Management: Increasing Resilience through Safety Assessment in SESAR. Proceedings of the Third SESAR Innovation Days. EUROCONTROL. http://www.sesarinnovationdays.eu/files/SIDs/2013/SID-2013-14.pdf

Woltjer, R., Pinska-Chauvin, E., Laursen, T., Joseffson, B. (2015). Towards understanding work-as-done in air traffic management safety assessment and design. Reliability engineering and system safety, In press

Woods, D. D. (2006). Essential characteristics of resilience. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.), Resilience Engineering: Concepts And Precepts (pp. 19–30). Aldershot, UK: Ashgate.

Woods, D. (2015). Four Concepts for resilience and the Implications for the Future of Resilience Engineering. Reliability Engineering and System Safety, http://dx.doi.org/10.1016/j.ress.2015.03.018

EXPERIENCES FROM HEALTHCARE: - SENSEMAKING

EXPLORING SYNERGIES BETWEEN THE DESIGN OF PROCEDURES AND THE DEVELOPMENT OF RESILIENCE SKILLS

Tarcisio Abreu Saurin[1], Priscila Wachs[2], and Marcelo Fabiano 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, Rua Barão do Rio Branco, 611-D-101, CEP 89801-030, Chapecó, Brazil
[1] saurin@ufrgs.br; Tel: +55-51-9628-2554
[2] priscilawachs@ig.com.br
[3] costella@unochapeco.edu.br

Abstract

While it is often taken for granted that gaps in procedures should be filled by well-trained workers, the identification of the most salient gaps and their training implications are not usually made explicit. This paper addresses this problem by introducing a framework for the identification of synergies between the design of procedures and the development of resilience skills (RSs). An instantiation of using the framework in a procedure of administering medications provides insights into its potential for the design of better procedures and training.

1 INTRODUCTION

The use of procedures and scenario-based-training (SBT) are well-known safety management practices in complex socio-technical systems (CSSs). On the one hand, procedures increase predictability and set a basis for the training of routine skills, which should be mastered even by novices. On the other hand, SBT supports the development of skills to deal with the variability that cannot be anticipated by procedures (i.e. resilience skills, RSs), which are usually mastered by experts. RSs are individual and team 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).

While it is often taken for granted that gaps in procedures should be filled by well-trained workers, the identification of the most salient gaps and their training implications are not usually made explicit. At least four reasons may help to understand this drawback. First, procedure application is not usually viewed as a substantive cognitive activity, but merely as rule-following. In this view, procedures are assumed to be applicable to all circumstances, and thus they are not supposed to have relevant gaps (Dekker, 2003). Second, popular methods for designing procedures originated from manufacturing industries characterized by repetitive tasks, in which motions and times of workers are specified in detail (e.g. Rother and Harris, 2001). Thus, there is a lack of empirically tested methods which fit to the dynamic nature of CSSs. Third, the design of training programs tends to follow the same assumptions and underlying logic of the procedures. Therefore, if procedures imply simple rule-following, training is likely to overvalue the need for following the rules, instead of developing awareness of possible gaps and the need for RSs. Fourth, the lack of concern with systematic ways of analyzing procedures can arise from narrow definitions of what counts as a procedure. Indeed, it is usually assumed that procedures mean action-oriented procedures, which specify in terms of if – then statements how people shall behave (e.g. wearing a seat belt when in a moving car) (Hale and Borys, 2013). This traditional view of procedures tends to be dominant among managers and regulators, and it also envisions procedures as being devised by experts, in advance, away from the time and production pressures of the front lines (Wears and Hunte, 2015).

However, goal-oriented and process-oriented procedures offer alternatives to action-oriented procedures, and these three types may be used in combination. While goal-oriented procedures define only what has to be achieved and not how it must be done, process-oriented procedures define the process by which the person or organization should arrive at the way they will operate – e.g. requirements to consult with defined people when an emergency situation arises in order to decide how to handle it (Hale and Borys, 2013). This paper partially addresses the aforementioned shortcomings by introducing a framework for the identification of synergies between the design of procedures and the development of RSs. An instantiation of using the framework in a procedure of administering medications provides insight into its potential for the design of better procedures and training.

2 A FRAMEWORK FOR INTEGRATING PROCEDURES AND SBT

The proposed framework for integrating the design of procedures and SBT assumes the preexistence of procedures and training programs in the organization, and therefore it could be better framed as a framework for system redesign. The framework has three stages: (1) the identification of RSs; (2) a content analysis of procedures; and (3) the identification of synergies between procedures and SBT. **Stage (1)** adopts the method proposed by Wachs et al. (2012), which uses techniques associated with cognitive task analysis (Crandall et al., 2006) – e.g. interviews, observations, and analysis of documents such as accident and incident forms. According to Wachs et al. (2012), RSs are used within a context, and therefore it is necessary to identify the work constraints that impact the RSs and the actions for system re-design facilitating their use. Furthermore, RSs are identified and classified across two levels of abstraction. Initially, they are identified at the less abstract level (referred to as examples of RSs), being extracted directly from the transcriptions of the interviews and documents. The search for evidence of RSs in the raw data is guided by identifying events in which workers had to adjust their performance to achieve their goals. While the resilience engineering literature does not define precisely what is meant by "adjusting performance", we propose it involves one or more of the following: (i) the insufficiency or absence of action rules; (ii) improvisation, which is defined by Trotter et al. (2013) as the real-time conception and execution of a novel solution to an event that is beyond the boundaries for which an organization has anticipated or prepared - therefore, improvisation assumes the insufficiency or absence of action rules; and (iii) the isolated existence of performance goals and/or process oriented rules. The second level of classifying RSs, referred to as RSs categories, is defined by labels, for each of which various examples are given. The choice of the labels that designate the categories is based on the assumption that employees should find them meaningful and easy to understand (Wachs et al., 2012).

The work constraints that have an impact on the RSs and that might be integrated into SBT are similarly organized. Extracting these constraints from the raw data is usually straightforward, since they are explicit in the events from which the RSs are extracted. At the less abstract level, constraints that can be incorporated into training scenarios (e.g. failure of certain equipment) are identified. At a more abstract level, labels are created for designating categories encompassing similar constraints (e.g. equipment failure). Concerning the actions for re-designing the system, these are not usually as explicit in the raw data as the work constraints. However, they can be inferred, since they often are the opposite of the constraints. For example, the constraint of equipment failure prompts the identification of maintenance improvement as a re-design measure (Wachs et al., 2012).

Concerning the content analysis of procedures (**stage 2**), it is based on eight criteria (Figure 1) developed from a literature review of types and schools of thought for designing procedures (e.g. Wears and Hunte, 2015; Hale and Borys, 2013; Dekker, 2003). This analysis should be carried out as a teamwork including employees directly involved in the task as well as both training and procedures designers. It is worth noting that although stage 2 stresses the *contents* of procedures, a broader and more effective evaluation should account for the whole process of *managing* procedures, which includes the processes of design and monitoring procedures. Some criteria proposed by Saurin and Sosa (2013) may be useful for this broader evaluation – e.g. procedures should be designed, reviewed and monitored by a team of representatives from all the areas affected by them. As a result of stage 2, gaps and improvement opportunities in the design of both procedures and training are identified. Such gaps and opportunities should be dealt with in **stage (3)**, in which both procedures and training programs should be redesigned to be complementary and aligned to each other, based on a resilience engineering approach.

We also propose that the application of the described method be framed as design science research (DSR), in which all or part of the investigated phenomenon (i.e. procedures and training) may be created as opposed to naturally occurring. The epistemology of DSR stresses knowing through making, and it is solution-focused, rather than problem-focused (Van Aken, 2004). This characteristic fits the nature of the problem addressed in this paper since the view of procedures simply as rule-following is likely to be predominant, in practice, over the view of procedures as substantive cognitive activity. Therefore, the investigation of the alternative view may need an intervention/redesign in the socio-technical system, in order to intentionally create the phenomenon to be investigated. Another characteristic of DSR is that the designed artifact is evaluated according to criteria that are made explicit in the awareness of the problem phase – some criteria may be those presented in Figure 1. Deviations from expectations are noted and must be tentatively explained. The theoretical connections and the research contribution of the solution, as well as its scope of applicability, should be exposed (Kasanen et al., 1993).

Criteria	Implications for the training of RSs
(a) Are the goals of the activity stated in the procedure?	As for the training of RSs, the statement of clear goals is important because it provides a basis for observing how trainees trade-off goals

(b) Are the minimum inputs and preconditions required to start the task stated?	The identification of the inputs and preconditions is crucial for the training of RSs. If these are not available, workers will have to make do using RSs to deal with scarcity of resources
(c) Are the work constraints that can make it difficult to follow the procedure stated?	Work constraints, such as the lack of the minimum inputs to start a task, push performance out of the design envelope, thus increasing the need for RSs
(d) Are there over specifications, or irrelevant specifications, that could be removed from the procedure?	Over specification would be detrimental for the training of RSs, since it would facilitate deviant performance that could be wrongly interpreted as worker´s violation. Furthermore, it would create double-binds for workers – e.g. either following the procedure and be blamed for not deviating when necessary, or not following the procedure and be blamed for deviating. As to irrelevant specifications, these can make the procedure unnecessary long and cumbersome
(e) Are the direct relationships with other procedures mentioned?	These relationships are important for SBT, since the lack of resources for carrying out an interrelated procedure is a work constraint that may demand RSs
(f) Are there examples of under / no specification that should have been specified?	Situations of unnecessary under/no specification possibly mean that RSs have been overused in detriment of routine skills
(g) Do situations identified from (f) have an impact either on safety or efficiency?	Unnecessary under/no specification increases the risk of undesired side-effects arising from the use of RSs
(h) To what extent is it possible and worth specifying the situations identified from (f)?	While some of the unnecessary gaps can be filled using action-oriented rules, others can be suitable for goal-oriented and process-oriented rules, as they rely on RSs to a greater extent. Moreover, the procedure could state the required RSs for steps associated with high variability, especially if there are either safety or efficiency implications

Figure 1. Criteria for analyzing procedures and implications for the training of RSs

3 AN EXAMPLE OF APPLYING THE FRAMEWORK

An application of the framework is illustrated by the procedure of giving medications to patients hospitalized in the emergency department (ED) of a University hospital. A case of healthcare was chosen since this environment is well-known for being highly complex, and therefore the limitations of viewing procedures as mere rule-following could be more salient. The data for the identification of RSs (stage 1) were originally collected for identifying RSs of three categories of professionals who worked in the ED (physicians, nurses, and nurses technicians), without emphasizing any particular internal process. Thus, although the data is also of interest for the task of giving medications, some nuances of that task were missed. In all, interviews were made with 20 employees, and about 100 hours of direct observations were carried out in the ED premises. The main results were: the identification of 97 examples of RSs (e.g. run patients in parallel, organize the work area in advance), grouped into 11 categories (e.g. re-plan the sequence of activities); the identification of 13 categories of work constraints that created the need for using the RSs (e.g. high number of patients); and the identification of 15 system re-design measures, which could either facilitate or reduce the need for using RSs.

The content analysis of the procedure (stage 2) was made as a class exercise (i.e. part of a 15h course on resilience engineering given by the first author of this paper) by twenty-five professionals who worked in the hospital; many of them worked in the ED. The professionals worked in groups and they prepared reports with their conclusions from applying the criteria. Figure 2 presents the main insights from stage 2 as well as some examples of synergies between the design of procedures and training, which correspond to **stage 3**.

Criteria	Results of the content analysis
(a) Are the goals of the activity stated in the procedure?	The procedure simply stated that the administration should be “safe and correct”. Professionals suggested that the “5 rights” should be explicitly mentioned
(b) Are the minimum inputs and preconditions required to start the task stated?	This information was fragmented over several sections of the procedure, and it focused on the materials for administering medications. Professionals suggested to group the inputs and preconditions into a specific section of the procedure as well as to include new ones
(c) Are the work constraints that can make it difficult to follow the procedure stated?	The procedure took for granted that ideal working conditions would be in place, and thus it did not mention any work constraint. However, data from stage 1 and reports by professionals indicated a number of constraints, such as the lack of prescriptions and high workload. Such work constraints and the RSs they require (e.g. “manage the time with each patient”) could be listed in the procedure and included in training sessions
(d) Are there over specifications, or irrelevant specifications, that could be removed from the procedure?	From the view of the professionals, no example of over specification was identified. Nevertheless, professionals identified sentences that were redundant or unnecessary – e.g. “bring the medications to the patient”

Criteria	Results of the content analysis
(e) Are the direct relationships with other procedures mentioned?	Professionals stressed that other procedures should have been referenced – e.g. the procedure of washing hands. Furthermore, RSs such as "anticipate the need for actions" may be necessary due to relations between procedures
(f) Are there examples of under / no specification that should have been specified?	Professionals indicated a number of unnecessary gaps in the procedure, such as: lack of guidance of how to identify whether the patient is able to swallow the medication; lack of information of where the administration of the medication should be recorded – the procedure only stated the need for the record, but not how to do this
(h) Do situations identified from (f) have an impact either on safety or efficiency?	All cited examples have an impact on patient safety – e.g. to give oral medication to a patient unable to swallow may cause an adverse event; lack of records of administered medications may cause the same medications being administered more times than necessary
(g) To what extent is it possible and worth specifying the situations identified from (f)?	Professionals indicated action and process rules that could fill most gaps – e.g. certain visual cues and questions should be made to the patient, in order to assess their ability to swallow. These cues and questions could be practiced in sessions of SBT

Figure 2. Content analysis of the procedure for administering medications

4 CONCLUSIONS

Both procedures and training can support the management of resilience, if designed from a resilience engineering viewpoint. Indeed, procedures too focused on action-rules and the resulting procedural training are of limited usefulness for resilience as they do not account for variability. By contrast, from the resilience engineering view the design of procedures is an opportunity for the design of resilient systems, which recognize that work-as-done in CSSs necessarily relies on RSs to some extent. Although an effective design of procedures must eliminate unnecessary complexity, a portion of complexity is unavoidable. This is not to say that the responsibility for being resilient fully rests on the shoulders of front-line employees. As stressed in stage (1) of the proposed framework, it is necessary to identify the work constraints that create the need for resilience at the front-line and to consider means of reducing these constraints and their impacts. Furthermore, the anticipation of the most salient gaps and the correspondent RSs upfront in the design of procedures is an example of being proactive in work system design.

The framework will be soon tested in a larger healthcare system, comprised by several inter-related procedures that can be simulated using SBT. It is expected that the use of the framework gives rise to a method for the design of innovative procedures conceived from a resilience viewpoint (i.e. resilient procedures). The Functional Resonance Analysis Method (the FRAM) will be used in order to identify the relations between the functions comprised by the procedures, which can provide insights into the design of both procedures and training. The FRAM is also envisioned as a tool for supporting the debriefing stage of SBT, in which trainees discuss the simulation under the instructor´s guidance. Last but not least, a systematic characterization of the complexity of the functions associated with procedures is expected to be useful, since this can shed light on the adequate balance mix of goal, process, and action-oriented rules. In principle, it is assumed that the lower the complexity of the function the greater the emphasis on action-rules.

REFERENCES

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

Dekker, S. (2003). Failure to adapt or adaptations that fail: contrasting models on procedures and safety. *Applied Ergonomics*, 34, 233–238.

Hale, A. & Borys, P.D. (2013). Working to rule, or working safely? Part 1: a state of the art review. *Safety Science* 55, 207-221.

Kasanen, E., Lukka, K. & Siitonen, A. (1993). The constructive approach in management accounting research. *Journal of Management Accounting Research,* Fall, 243-264.

Rother, M. & Harris, R. (2001). *Creating Continuous Flow*: an action guide for managers. Lean Enterprise Institute, Cambridge, MA.

Saurin, T.A., Wachs P., Righi, A. & 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.

Saurin, T.A. & Sosa, S. (2013). Assessing the compatibility of the management of standardized procedures with the complexity of a sociotechnical system: case study of a control room in an oil refinery. *Applied Ergonomics*, 44, 811-823.

Trotter, M., Salmon, P. & Lenné, M. (2013). Improvisation: theory, measures and known influencing factors. *Theoretical Issues in Ergonomics Science*, 14 (5), 475-498.

Van Aken, J.E. (2004). Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules. *Journal of Management Studies* 41 (2), 219 – 246.

Wachs, P.; Righi, A. & Saurin, T.A. (2012). Identification of non-technical skills from the resilience engineering perspective: a case study of an electricity distributor. *Work*, 41, 3069-3076.

Wears, R. & Hunte, G. (2015). *Resilient procedures - oxymoron or innovation*? In: Braithwaite, J., Wears, R. & Hollnagel, E. (Eds.), Resilient Health Care III: Reconciling Work-As-Imagined and Work-As-Done. Ashgate, in press.

SUPPORTING PROSPECTIVE SENSEMAKING IN AN UNPREDICTABLE WORLD

Ragnar Rosness[1], Torgeir Haavik [2] and Tor Erik Evjemo[3]
[1,3] SINTEF Technology and Society, P.O. Box 4760 Sluppen, NO-7465 Trondheim, Norway
[1] Ragnar.Rosness@sintef.no, [3] TorErik.Evjemo@sintef.no
[2] NTNU Social Research Ltd., 7491 Trondheim, Norway
[2] Torgeir.Haavik@samfunn.ntnu.no
www.sintef.no www.samforsk.no

Abstract

We studied the role of sensemaking processes in the safe and efficient performance of surgical procedures. The study is based on observations, semi-structured interviews and informal conversations with surgeons, anaesthetists, operating nurses and anaesthetic nurses. The members of the operating team paid great attention to what might happen during the next seconds, minutes and hours. They thus built a capacity for anticipation which enabled them to collaborate smoothly and prepared them to handle undesired but foreseeable occurrences. We label this activity "prospective sensemaking" and argue that it is a precondition for safe and successful completion of surgical procedures. Instead of waiting for things to happen and making sense of them in retrospect the operating team members constructed plausible projections of what might happen and how they might handle such plausible futures. We discuss how procedures and technology may support prospective sensemaking. In this way, the paper points to resilience strategies that are compatible with the values and capacities of operating teams and that make good use of their current resources and capacities.

1 INTRODUCTION

This paper is based on a study of the role of sensemaking processes in the safe and efficient performance of surgical procedures. Working in a surgical team within an operating theatre involves relying on a variety of roles, procedures and technology. The varying entities within an operating theatre, not least the patient, are complex and interlaced, which means that different types of surgery include elements of unpredictability of varying degrees (Rosness et al., in review). We found that the members of the operating team paid great attention to what might happen during the next seconds, minutes and hours. They thus built a capacity for anticipation which enabled them to collaborate smoothly and prepared them to handle undesired but foreseeable occurrences related to patient status. We label this activity "prospective sensemaking". Instead of waiting for things to happen and making sense of them in retrospect, the operating teams constructed plausible projections of what might happen and how they might handle such plausible futures.

Although our approach to sensemaking is highly influenced by Weick (1995), we investigate aspects of sensemaking that are distinguished from those Weick emphasised in two regards: First, while we do acknowledge that sensemaking is a social process, we also include procedures and technology in our analysis. Secondly, our study of sensemaking also covers situations that Weick characterises as non-events. These are situations where operations progress in a smooth and safe manner. We claim, however, that the operations pass smoothly and safely not because little happens, but because much happens. Our study was rigged to capture the *dynamic events* – supported by social and technological resources – that are suggested to be central ingredients of prospective sensemaking. Our approach to sensemaking and the distinctions we make between retrospective sensemaking and prospective sensemaking can thus be related to the distinction between Safety I and Safety II (Hollnagel, 2014); rather than being occupied primarily with those situations where things obviously break down and must be explicitly handled, we devote attention to what happens when apparently nothing happens, when operations proceed smoothly and the outcome does not evoke anyone's attention.

Traditionally, when one has managed patient safety the idea has been to adopt safety solutions from other industries relying on perspectives such as quality management, lean production, and high reliability organizing). However, in order to improve the quality of health care and patient safety in particular, health care needs to focus on its ability to deal with the unpredictable through various ways of adapting (Hollnagel et al., 2013). Our aim was to study teamwork practices during naturally occurring surgical procedures in line with one of the main premises of Safety-II (Hollnagel, 2014), to understand how a system is able to succeed under varying conditions by focusing on the nature of everyday clinical work as it is done (Hollnagel et al., 2013). This paper also contributes empirically to knowledge on one of resilience engineering's four cornerstones, namely anticipation (Holnagel et al., 2011) and how one at the sharp-end actually is able to know what to expect as the surgical intervention proceeds. This paper

describes the characteristics of prospective sensemaking (Rosness et al., in review) in the operating theatre and discusses how technology and procedures can further support (and strengthen) this phenomenon. The paper also discusses implications for training the various roles in the operating theatre.

The study is based on observations, semi-structured interviews and informal conversations with surgeons, anaesthetists, operating nurses and anaesthetic nurses.

2 THE NOTION OF "PROSPECTIVE SENSEMAKING"

The notion of "prospective sensemaking" may be viewed as an elaboration of aspects of sensemaking that received limited attention in Weick's (1995) conceptualisation of sensemaking in organisations. According to Weick, the term "sensemaking" means what it says, i.e. the process of making sense. He conceptualised sensemaking as a social process rather than an individual, cognitive process. According to Weick sensemaking is typically triggered by uncertainty or ambiguity. He further suggested that sensemaking is a retrospective process in the sense that actors look back on what has happened to make sense of the current situation (Weick, 1995, p. 24-30). It is also retrospective in the sense that actors look back on their previous words and actions to make sense of them.

We define "prospective sensemaking" as sensemaking processes where the attention and concern of people is primarily directed at events that may occur in the future. The qualification "primarily" is necessary because, even when our main focus is on possible future events, we may draw on past experience to make sense of the future, and thus attend to the past as well.

Based on our observation and on interviews and informal conversations with members of the operating teams we propose the following characteristics of prospective sensemaking (Rosness et al., in review):

The persons involved are primarily concerned with their own and the team's successful handling of events in the near or intermediate future, ranging from seconds and minutes to weeks and months into the future. Their attention is thus directed at the future, rather than the past.

Prospective sensemaking does not necessarily require strong external cues or triggering events to occur. While retrospective sensemaking activities are typically triggered or intensified by uncertainty or ambiguity, prospective sensemaking also occurs spontaneously, as a "natural" part of the work practice.

Prospective sensemaking relies on both verbal and non-verbal communication, including observation of the actions of others and of the effects of those actions.

Prospective sensemaking can be open to the possibility of alternative chains of events – the future may be conceived as an event tree rather than a single path of events. An implication of this is that prospective sensemaking allows for ambiguity and uncertainty.

The main outcomes of successful prospective sensemaking are practical preparations to handle possible future events, mental preparedness to interpret future events and improved coordination in tasks involving intertwined actions of two or more persons.

The process of prospective sensemaking may involve human as well as non-human actors, including different forms of representations or models.

A straightforward argument for the importance of prospective sensemaking for the safe and efficient performance of surgical procedures can be made by considering how the performance of a surgical procedure would proceed if the operating team did *not* engage in prospective sensemaking. The time to complete surgery would increase because the scrub nurse would not have the correct tool ready at hand; the surgeon would repeatedly have to wait for the ambulating nurse fetching tools and materials; the patient would be at risk of experiencing pain while under general anaesthesia because the anaesthetic nurse would be unable to adjust the distribution of painkiller prior to strong pain stimuli, etc. Prospective sensemaking can also be crucial for the maintenance of organisational structure, since confidence in leaders tends be destroyed if organisation members are not able to make sense of their leaders' actions (Weick, 1993). Participants in the study confirmed that they had experienced significant variations in the effectiveness of prospective sensemaking in operating teams, and that ineffective prospective sensemaking did lead to inefficient performance and a general sense of unease in the operating team. They said that this state was most likely to occur when members of the operating team were unfamiliar with the surgical procedure or when the surgeon failed to communicate clearly about the expected course of the operation.

3 PROCEDURES

We observed several ways in which procedures supported prospective sensemaking in conjunction with the surgical interventions.

The Safe Surgery Checklist ("Trygg kirurgi"; Høyland et al. 2013) checklist prescribes items to be checked and information to be shared at three different milestones during a surgical intervention. This is a generic checklist, common to a diversity of surgical interventions. This checklist provided an opportunity to recover from errors such as omissions, misunderstandings and incorrect information. Moreover, by providing a timeout, the checklist encouraged exchange of information, concerns and requests even beyond the items specifically mentioned in the checklist. In a feedback meeting, after we had presented the notion of "prospective sensemaking", a surgeon commented that the Safe Surgery Checklist supported prospective sensemaking because it promoted sharing of information that the other members of the operating team needed to foresee what might happen during the surgical intervention.

Several operating nurses mentioned that they had procedures covering the specifics of each surgical procedure, for instance what tools, materials and equipment should be prepared. These procedures helped prospective sensemaking by outlining the expected course of the surgical intervention as well as some possible contingencies, and by prescribing the tools and equipment to be prepared for each intervention. However, some operating nurses mentioned that surgeons in some cases preferred to use tools or equipment that deviated from the standard procedure, and that they might call the surgeon the day before the surgery to check for such preferences.

A surgeon told us about how he prepared for an operation. He insisted that a surgical intervention is by definition planned in advance. The master plan can, however, be made up of several sub-procedures. He usually has a "plan B" and perhaps a "plan C" ready at hand because he may not know which plan will be optimal before the intervention starts. Because the surgeon made up a "plan B" and perhaps a "plan C" in advance, preparations could be made for different courses of the surgical procedure. The nurses would prepare instruments and equipment for carrying out "plan B and C" as well as "plan A". This would allow the operating crew to change smoothly form "plan A" to "plan B" if need be. A prerequisite for this smoothness was that the procedures used by the operating nurses corresponded in scope to the procedures referred to by the surgeon. The procedures served as black boxes, which allowed for effective communication about combinations of several alternative and intrinsically complex courses of the surgical intervention.

To summarise, procedures may support prospective sensemaking (1) by creating a timeout and cues for exchange of information, concerns and requests, (2) by outlining the expected course of the intervention and prescribing the preparations, and (3) by providing building blocks for devising a robust master plan for the surgical intervention.

4 TECHNOLOGY

A series of representational tools entered into the work of making sense of current and future states of the object of investigation; visualisations based on microscope, X-ray, Computer Tomography, Magnetic Resonance and ultrasound were all used actively to evaluate and negotiate current and future states and thus to expand and articulate the border between the known and the unknown. This, we argue, serves as useful input to inform the team about where the limit goes between necessary adaptation and risky deviation.

One example of this was an operation of a benign tumour on the pituitary gland. A central challenge in this operation was to draw the line between what tissue to remove and what to leave behind, thus determining when to stop operating. Often, this will correspond to the border between healthy and sick tissue. In this case, however, pragmatic concerns made the border between what tissue would exert pressure on the visual nerve and what would not as the relevant border. Should too little be removed, the tumour would still exert pressure on the visual nerve. Should too much be removed, then neurological side effects might occur.

Being inaccessible to the naked eye, the tumour had to be enacted through a series of representations produced by a series of tools (microscope, X-ray, MR, ultrasound). Through these tools and the practices accompanying them, the ontological status of the tumour as an object was gradually strengthened. As explained towards the end of this section, the ontological status makes a difference since it is central in producing the ad-hoc border that eventually will count as a pragmatic stop criterion to the surgeon. While MR images are taken *before* the operations and thus serve as a point of reference, X-ray images are taken *occasionally during* the operation for the purpose of navigating. Ultrasound images are created and discussed in *real time*, in an attempt to distinguish the tissue to be removed from the tissue to be left untouched while the surgeon is working, with the direct impact this will have for the result of the operation and the patient's vision in the future.

Consider the following extracts from different stages in the operation:

The ultrasound technician refers to the screen where the microscope image is projected: “What is that white thing?” Surgeon: “I don’t know”

After a while, the doctor says loudly to everybody in the room (who can see on two different screens what he sees in the microscope): “I wonder if that is the pituitary gland we see there…”. He walks over to the screen in the corner again, where he discusses with the technician: “Should we try and see if we can see anything on the ultrasound?” He starts walking back to the operation table, when he is called back by the technician, who points to the screen: “Be aware of those blood vessels… come here and see.”

The ultrasound technician and the surgeon discuss the ultrasound images and try to sort out what is tumour and what is healthy tissue, and implicitly when to stop operating. More images are taken. More discussion. They can see the tumour, but they note that there is not much manoeuvring space to access it. They walk together back to the MR image displayed on the PC in the corner. The discussion at this point integrates three highly mediated representations that, together with the microscope images, amount to the final representational state that is worked upon.

During the next few minutes, the doctor demonstrates the craftsmanship of surgery, partially removing the tumour with basic tools (forceps and scalpels), followed by the production of some final ultrasound images. As the surgeon told us after the operation, the border between sick and healthy tissue is not easy to establish clearly, and sometimes it is not what defines the stopping criteria either. Thus, in absence of a de facto border, the border should be thought of as a pragmatic border, constructed by aid of representational technology in combination with considerations about future implications for the patient's vision.

The significance of *shared representations* for prospective sensemaking was exemplified by the operating microscope. The microscope supported prospective sensemaking by providing a dynamic real-time representation, which was shared by and made intelligible to the whole operating team. The scrub nurse, the ambulant nurse and the anaesthetic nurse used this shared representation to update their conception of what was happening and what could happen in the near future.

Image-producing technologies may also have unintended effects. The heavy instrumentation in the operating theatre produces a lot of noise. This made our observation more difficult, since it was sometimes hard to hear what people said to each other. The noise may also disturb the team's communication. Another possible effect of the technologies is that they may generate additional workload and draw attention away from phenomena that may be more important at certain moments. These are general consideration that we have not focused on in this study, but that would certainly be worthwhile to explore in other studies.

5 DISCUSSION: HOW TO SUPPORT PROSPECTIVE SENSEMAKING

Although we characterise prospective sensemaking as anticipation, we do not suggest that prospective sensemaking is about anticipating the future as it will actually unfold. Rather than expecting the unexpected, or imagining the unimaginable, prospective sensemaking actualises *possible* futures that may or may not occur. Thus, it works as an elaboration of potential future states that one may prepare for. By elaborating on potential future states prospective sensemaking helps articulate the domain of the expected and by that drawing visible borders towards the unexpected. One central challenge of resilience is that the necessity to sometimes operate outside the prescribed work practices is problematic since one often does not know how far from the prescriptions it is justifiable to go. One way of talking about this is to say that one does not know when the border for safe operations (as portrayed by Rasmussen, 1997) is crossed, since this border usually is made visible only in retrospect. The border between the domain of the known and the terra incognita, however, may be operationalised through prospective sensemaking. A central ingredient of prospective sensemaking is to articulate this border by actualising potential futures.

Our notion of "prospective sensemaking" may to some extent coincide with the notion of "anticipatory thinking" proposed by Klein et al. (2010). Klein et al. characterise anticipatory thinking as a "future-oriented aspect of sensemaking". The difference between the two concepts appears to be more in style of conceptualisation than in the phenomena they seek to capture. Klein et al. conceptualise "anticipatory thinking" in terms of postulated cognitive functions that apply to both the individual level and the group level. We developed the notion of "prospective sensemaking" in an abductive manner from a study of everyday practices in the operating theatre, using techniques associated with grounded theory. "Prospective sensemaking" emerged from this analysis as a promising core category, with a capacity to integrate a broad range of findings from the interviews and observations. Following Weick, we think of sensemaking as an intrinsically social process. We prefer the term "sensemaking" because it hints at the interplay with retrospective sensemaking (Weick, 1995), and because in everyday language "thinking" is usually associated with covert cognitive process at the individual level. Another contrast with the style of theorising of Klein et al. is that we prefer to suspend normative judgements on whether

prospective sensemaking is "correct" or "false". When discussing barriers to anticipatory thinking, Klein et al. seem to contrast fallible thinking in the real world with a normative ideal of rational logical thinking.

We found that procedures may support prospective sensemaking in several ways:

1. As illustrated by the Safe Surgery Checklist, a procedure may help to create a timeout for checking that necessary preparations had been carried out and for exchange of information, concerns and requests and provide a structure for this information exchange.
2. Procedures specific to each surgical intervention and to the role of the operating nurses outlined the course of the intervention and prescribed the preparations to be made.
3. Procedures may be used as building blocks for devising a robust master plan for the surgical intervention. Such master plans may include two or more alternative trajectories, one of which may subsequently be selected based on findings during the intervention. This master plan provided an effective means to communicate the surgeon's expectations and the need for materials and equipment to the operating nurses.

Our results suggest that the utility of the procedures may be enhanced when they are used in a flexible manner that is compatible to the constraints of the task (Grote 2008). The utility of the Safe Surgery checklist was enhanced by team members providing information or raising concerns beyond those specifically mentioned in the checklist. The operating nurses introduced some flexibility into the procedural control of surgical interventions by checking if the surgeons had specific preferences and by combining two or more procedures in cases when the surgeon needed the flexibility to change plans during the intervention.

Prospective sensemaking is also supported by representational technologies; both microscopes and 3D ultrasound apparatuses are examples of technologies that provide dynamic real-time representations that are not only available to the surgeon, but to the whole team. These representations are used to make sense of current and future states, both collectively as shared understanding, and less convergent as boundary objects (Star and Griesemer, 1989) offering different (not in the sense contradictory) meanings to different actors.

Can training contribute to effective prospective sensemaking? Operating nurses participating in our study told us that there were considerable differences between how surgeons communicated about the progress of the intervention, whereas a surgeon told us that practices to enhance prospective sensemaking were not part of their training. Rather than training "non-technical skills" as a separate add-on, it might be worthwhile to seek ways to train practices supporting prospective sensemaking as an integrated part of the basic training of health professionals. This might include training prospective operating nurses and anaesthetic nurses skills related to sharing information, raising concerns, and "reading the situation" based on non-verbal cues.

Advances in information technology and visualisation the later years have had a profound effect on how one thinks about and seeks to arrange for collaboration in complex, information dense and risk-prone operations. Integrated Operations (IO) in the petroleum industry may serve as one example; IO is an operating philosophy where greater use of real-time data and stronger integration across geographical locations and professional disciplines is expected to enable faster, better and safer operations (Albrechtsen and Besnard, 2013). The point here is not to focus on the efficiency measures, but on the technology that supports sensemaking and collaboration. Central resources in that operating regime are representations and visualisations that are shared by geographically distributed teams. These representations and visualisations may refer to current states of affairs, or they may be constructed models that refer to potential future states or safe limits for those. We have witnessed several initiatives of research and development collaboration between the health domain and the petroleum domain in order to share knowledge on these issues. Without going into detail on how representation and visualisation tools may support not only desired processes, but also support undesired processes, or anti-tasks (Turner, 1978), we may establish that they are acquiring an increasingly central role in the operation theatre.

6 CONCLUSION

In order to manage resilience we need to understand the strategies, techniques and resources people use to anticipate and handle unlikely but foreseeable consequences. We have labelled observable aspects of this process "prospective sensemaking". Technological means (including procedures) may support prospective sensemaking in several ways: (1) by prescribing, legitimising and structuring sensemaking activities; (2) by directing the work through engineered work processes, making projections of what is to happen in the future easier; (3) by providing building blocks for devising and sharing master plans with alternative trajectories; (4) by providing shared and continuously updated information, thus facilitating coordination; (5) by establishing boundaries between the known and the unknown; (6) by providing continuously updated information combined with projections of

expected and/or desired future states, indicating deviations from expected or desired trajectories at a sufficient early point in time to make necessary corrections.

Acknowledgements

This research was funded by the *Center for Integrated Operations in the Petroleum Industry,* Norway. The study was made possible by collaboration with *Operating Room of the Future, St. Olavs Hospital, Trondheim University Hospital* (FOR – "Fremtidens operasjonsrom"). FOR was a partner in the project. They introduced us to the two surgical departments and gave us access to their research infrastructure during the project period

REFERENCES

Albrechtsen, E. & Besnard, D. (2013). Oil and Gas, Technology and Humans: Assessing the Human Factors of Technological Change. Farnham: Ashgate.

Grote, G. (2008) Rules management as a source for loose coupling in high-risk systems. In E. Hollnagel, C.P. Nemeth & S. Dekker (Eds.) Resilience Engineering Perspectives. Volume 1: Remaining Sensitive to the Possibility of Failure (pp. 91-100). Aldershot: Ashgate.

Hollnagel, E. (2014). Safety-I and Safety-II: The Past and Future of Safety Management. Farnham: Ashgate.

Hollnagel, E., Pariès, J., Woods, D. & Wreathall, J. (2011). Resilience Engineering in Practice: A Guidebook. Farnham: Ashgate.

Hollnagel, E., Braithwaite, J. & Wears, R.L. (2013). Resilient Health Care. Farnham: Ashgate.

Høyland, S., Aase, K., Hollund, J.G. & Haugen, A.S. (2013) What is it about checklists? Exploring safe work practices in surgical teams. In C. Bieder & M. Bourrier (Eds.) Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization? (pp. 121-138). Farnham: Ashgate.

Klein, G., Snowden, D. & Pic, C.L. (2010). Anticipatory thinking. In K. Mosier & U. Fischer(Eds.), Informed knowledge: Expert performance in complex situations. London: Psychology Press.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. Safety Science 27, 183-213.

Turner, B.A. (1978). Man-made disasters. London: Wykeham.

Rosness, R., Evjemo, T.E., Haavik, T. & Wærø, I. (in review). Prospective sensemaking in the Operating Theatre. Article manuscript submitted to Cognition, Technology & Work.

Star, S.L. & Griesemer, J.R. (1989). Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. Social Studies of Science 19, 387-420.

Weick, K.E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. Administrative Science Quarterly 38: 628-652

Weick, K.E. (1995) Sensemaking in organizations. Thousand Oaks: SAGE.

DIALOGIC SENSEMAKING AS A RESOURCE FOR SAFETY AND RESILIENCE

Garth S Hunte [1], Christiane C Schubert [2] and Robert L Wears [3]
[1] Department of Emergency Medicine, University of British Columbia,
910 West 10th Avenue, Room 3300, Vancouver, BC, Canada V5Z 1M9
[1] garth.hunte@ubc.ca
[2] School of Medicine, Loma Linda University,
24760 Steward Street, Room 4203, Loma Linda, CA, USA 92350
[2] cschubert@llu.edu
[3] Department of Emergency Medicine, University of Florida,
655 W 8th Street, Jacksonville, FL, USA 32209
[3] wears@ufl.edu

Abstract

Dialogic theories provide an approach to understanding interaction, and include the perspective that human sensemaking is action-based, contextual, and constituted in interdependent relations with 'the other'. Hence, intersubjectivity is the defining property of communication. Sensemaking 'on-the-fly' takes place in parallel with evolving operational action. Shared (social) sensemaking creates and nourishes common awareness and understanding of the 'operating point', and in so doing facilitates coordination and safer performance. This is an essential condition for the emergence of safety and resilience. Practitioners, therefore, must have a way to meaningfully collaborate and make sense of what is going on. Dialogism, in this context, offers an opportunity for practitioners with different logics and perspectives, to meet, engage, and allow for something generative to happen. In this way, dialogic sensemaking provides a resource for resilience, by enabling a shared awareness of 'the sense of the event' (*phronesis*) and a collective response to the actual and potential.

1 INTRODUCTION

Safety and resilience emerge out of dynamic socio-technical interactions embedded in shared and contested practice [Dekker (2005), Hunte (2010)]. Creating safety and resilience is something we *do* – everyday. Safety – as action in practice – is a dynamic and distributed construct transmitted in stories [Cook et al. (1998), Iedema et al. (2006a), Rochlin (2003), Sanne (2008)], and the stories we tell one another about everyday practice (successful and unsuccessful) facilitate reflection, sensemaking, and learning [Weick (1995)].

- I can only answer the question "What am I to do?" if I can answer the prior question "of what story or stories do I find myself a part?" [MacIntyre (2007), p. 216].

Thus, approaches to safety, like resilience engineering, must be based on accounts of *work-as-done* to afford a dialogue for learning. In this paper, we discuss an everyday example from healthcare – interaction between physicians and nurses in care of a patient – and argue that dialogic sensemaking is a resource for resilience and safety.

2 INTERACTION

Interactions in a hospital emergency department (ED) are complex; communication is often chaotic and brief, with multiple interruptions, and transitions [Hunte(2010)]. For example,

- An elderly patient was brought to an ED by ambulance having been found collapsed and vomiting in the washroom of a public building. Almost 40 minutes later, the bedside nurse (Nurse A) comes to tell the Clinical Nurse Leader (CNL) that the patient "not to be confused with the other patient with the same last name" is to be transferred to the trauma room "decreased [level of consciousness], very hypertensive, and starting to do the 'neuro'". However, the patient had recently received Gravol, and Nurse A wonders if "his [level of consciousness] is decreasing or if it's the Gravol?" Nurse A and the CNL go over vital signs and medication as they arrange to move another patient (recently cardioverted and bradycardic) out of the trauma room in order for this patient to be moved in.

- It is also shift change for the emergency physicians: emergency physician A (EPA) is leaving, and emergency physician B (EPB) is arriving). Respiratory therapy is paged, and the clinical educator is available for support. EPB and the emergency resident are "running the show". Verbal orders are given to the trauma nurse (Nurse B) for some medication, and EPB states "I put this all in the computer".As

> the patient is being prepared for intubation, nurse A approaches the CNL with her concern that this is "overkill". The CNL queries EPB and the emergency resident about the chemstrip (normal) and if narcan had been given (no). EPB states "we're going to go with thiopental, midazolam and [succinylcholine]". EPA enters the room and nurse B asks "how much midazolam?" EPA responds "Fentanyl, thiopental, and sux". Four minutes later, while drawing up the other medication, nurse B looks at the order sheet and asks "I've got an order for midazolam, but was asked to pull up fentanyl". The confusion was clarified, the patient medicated and intubated. There was no harm. The patient was eventually diagnosed with an intracranial hemorrhage and transferred to neurosurgery.

The care providers in this everyday example attempt to make sense of the situation, but do not share their perspectives directly with each other. This lack of interaction leads to conflict and confusion, and poses a threat to patient safety. Although no harm was suffered in this event, the case illustrates the need for increased interaction, communication, and shared sensemaking.

3 DIALOGIC SENSEMAKING

Dialogic storying provides a theoretical approach to understanding interaction [Boje (2008)]. Dialogic theories include the perspective that human sensemaking is action-based, interactional and contextual, and constituted in interdependent relations with "the other" [Linell (2009)]. Human activity is mediated by the use of material and cognitive artifacts, wherein interactions and situations, as the foundation for dialogue, are the primary substrates for discourse. Therefore, the coordinated use of tools and signs shape all joint activity, including communication, collaboration, and collaborative problem solving [Wells (2007)].

3.1 Intersubjectivity

Action, communication, and cognition are thoroughly relational, interactive, and deeply embedded in social and cultural contexts. As such, interaction is both locally situated and shaped by sociocultural practices. The delicate connection between the subjective, individually experienced reality with the objective social reality (sustained over time as social facts) gives rise to the important, yet complex concept of intersubjectivity[3] [Eden (1981)] as the defining property of communication [Habermas (1970)]. Linguistically, "every word is directed towards an answer and cannot escape the profound influence of the answering word that it anticipates" [Bakhtin (1981), p. 280]. Understanding *in situ* is therefore related to the ability to anticipate and respond.

3.2 Narrative

Human understanding is fundamentally based on narrative [Bruner (1991)], and meaning making is pragmatically attuned to social context. The complexities of work and work relationships can be reflected in storying [Boje (2008)] – particularly dialogic stories – which allow for nonlinear understandings [Herman (2002)], and encompass multiple perspectives, tensions, and contradictions [Bakhtin (1981)]. Rochlin (2003) posits that a collective commitment to safety is an institutionalized social construct. Stories and rituals transmit operational behaviours, group culture and collective responsibility. The dynamic, inter-subjectively constructed narrative is one of organizational rather than individual performance.

4 ORGANIZATIONAL LEARNING

It is common to think of learning in organizations as a form of knowledge acquisition and to relate it to instruction and training. From this 'banking model' perspective [Freire (1993)], learning amounts to the acquisition of data 'out there' to be acquired and stored in the 'container/compartment' of the mind, implying a separation between actor and context [Gherardi (2002)]. This is the model followed by classroom safety instruction and admonishments and prescriptions about what is and is not safe. Safety learning tends to be in the form of more education, and more underspecified rules and procedures, rather than engaging the learner in situated practice.

4.1 Situated learning

An alternate relational perspective presents the image of learners as social beings who construct their understandings and learn from social interaction within specific socio-cultural settings [Suchman (1987), Engestrom (1987), Lave & Wegener (1991)]. Learning is viewed as the historical production, transformation and change of people: learning is no longer equated with simple appropriation or acquisition, but is "understood as

3 The sharing of subjective states by two or more individuals.

the development of a new identity based on participation in the system of situated practices" [Gherardi (2002), p. 193]. Learning is thus conceived as a way of taking part in a social process mediated by artifacts, not as a cognitive way of coming to know [Lave & Wegener (1991)]. These ideas are further enriched by views of power [Law (1986)], by emphasis on networks of human and non-human 'actants', such as computers [Fox (2000)], and by looking to the transformational nature of collaborative endeavours [Blackler (2000)].

4.2 Sensemaking

When human agents try to make sense of what is happening, they begin from some place, perspective, or viewpoint – their *habitus* [Bourdieu (1977)]. Perception is enacted [Merleau-Ponty (1962), Noe (2004)]. Schema guide perception and inference [Fiske (2008)], and assign significance and meaning. Options for data that do not fit the current frame include elaborating or preserving the frame (explain away the data), which is what novices frequently do [Schubert (2013)]. Another option for data that do not seem to fit is to seek an alternate frame (reframing). Hence, data mandates frame adjustment or change, and the basic sensemaking act is data-frame symbiosis [Klein (2006a, b)].

For example, early consideration of a hypothesis (rapid frame recognition) permits both more efficient data gathering and more specific expectancies which prompt adjustment or reframing if violated. Effective problem solvers differ from other approaches by using diagnostic frames to interpret data, but remaining willing to discard them when confronted with disconfirming data (reframing when the data no longer fit the frame) [Rudolph (2003)].

Sensemaking 'on-the-fly' takes place in parallel with evolving operational action [Albolino (2007)]. Shared (social) sensemaking creates and nourishes common awareness and understanding of the 'operating point', and in so doing facilitates coordination and safer performance [Cook (2005)]. Storytelling and dialogue create awareness of the character of coming events because narrative is subject to practical wisdom. As such, they allow for the expression of a normative stance or may guide the resolution of conflict between norms [Kirkeby (2009)].

4.3 Transitions

In healthcare, for example, two key aspects and challenges of collaborative care are transitions and team coordination. Shared sensemaking is required to build the understanding needed to inform and direct actions to address the hazards that threaten safety [Battles (2006)]. Transitions, such as patient hand-overs, involve much more than monologic information transfer; they also include a transfer of control or responsibility [Cohen (2010)]. As such, they present opportunities for sensemaking and resilience [Patterson (2010). In addition, the distributed and uncertain nature of everyday clinical work calls for flexibility in structuredness and degree of interaction at transition points [Behara (2005)]. Hence, standardized 'one-size-fits-all' communication scripts (for example, SBAR) that are frequently implemented to guide information transfer in clinical settings are limited in ability to facilitate dialogic sensemaking.

4.3 Safety narratives

Organizational safety narratives are constructed in stages [Waring (2009)]. Initially, practitioners interpret risk embedded in context, and give accounts that are intersubjective in character, and often emotionally rich. Such localized meanings of risk reflect wider assumptions about responsibility, culpability, and blame. These storied accounts are then re-constructed as written reports, where 'narrow narratives' are created to match pre-defined taxonomie, then further re-constructed through routine risk management perspectives, where accounts are re-coded and translated. Hence, the experiential, qualitative and culturally rich stories of practitioners are largely transformed into the abstract, quantitative, explicit, and often legal variables of management. While this process may benefit risk management, it destroys context, and devalues the affective and interpersonal knowledge of practitioners to the extent that they may only report those safety events that 'fit' the prescribed model. As such, practitioners are discouraged from reporting more complex or ambiguous events, despite important safety implications. It follows then that the mismatch between complex stories and the simplifying constraints of a reporting system can impede rather than enhance learning.

Individuals and groups 'make sense' of and interpret their experiences through storying [Boje (2008), Iedema (2006a), Waring (2009)]. Stories about safety incidents are developed within the interactions of practice, and reflect a dynamic mix of emotion and shared notions of responsibility [Waring (2009)]. Importantly, stories are woven together through social interaction, thereby reflecting inter-subjective and wider cultural beliefs. Thus, stories help to establish and reinforce collective sensemaking, especially in situations of uncertainty [Weick (1995)]. The narrative perspective is also attentive to the links between knowledge and power, in recognizing that storytelling provides a basis for defining social reality, and the privileging of particular forms of social action

[Foucault (1980)]. In this way, the notion of dialogic sensemaking provides a resource for resilience, by enabling a shared awareness of 'the sense of the event' (*phronesis*) [Kirkeby (2009)] and a collective response to the actual and potential [Hollnagel (2009a)].

5 RESILIENCE

Resilience describes the resourcefulness generated from the affordances of the work context [Woods (2006)]. Resilience in anticipating and recovering from threats to operational performance and safety is dependent upon the improvisation and sensemaking of practitioners in dialogic and distributed action [Hutchins (1995), Cohen (2006)]. Active sharing and updating of sensemaking, through the practice of 'heedful interrelating' {Weick & Roberts (1993)], enables risks to be collectively and progressively monitored [Boreham (2000)]. Similar to jazz improvisation, or *bricolage*, skillful communication and sensemaking can be assessed by the degree to which conversational moves simultaneously follow what has transpired previously and enable others to follow and facilitate forward movement in the meaning-making process [Weick (1995), Zack (2000)].

5.1 Stories of practice

Sharing and co-creating stories in a community of practice facilitates system learning and resilience [Perry (2009)]. Post-bureaucratic 'bottom-up' techniques that engage clinicians in teleo-affective[4] and dialogical narratives creates a space for "operationalizing concerns, emotions and judgments ... and privileges discourses that give greater prominence to what matters to those who do the work" [Iedema (2006a), p. 142]. Stories of practice become living practical theories that help practitioners make sense of their professional lives [McNiff (2007)], as well as guide their approach in routine and novel situations where uncertainty and risk are high.

All stories are perspectival, and told from a situated viewpoint. Hence, multiple tellings from different perspectives affords the greatest opportunity for co-creating a complex and nuanced picture of what happened [Cook (1998)]. Therefore, the quest for safety includes the search for multiple viewpoints [March (1991)]. A forum of conflicting views of safety is an essential prerequisite for enhancing an organization's potential for learning [Westrum (1993)]. A culture that influences safety positively is thus not necessarily one which is homogenous or conflict free, but one in which there is enough space to deal with conflict wholistically [Schubert (2008)]. This implies that conflict is dealt with in a constructive, democratic manner with equal consideration of all stakeholders [Antonsen (2009), Schubert (2008)]. Therein lies the need for dialogic interaction.

Even as every human being acts with a view to some good, so too the purpose of the organization is to create value [Nonaka (2007)]. Leaders in organizations with collective *phronesis* develop shared practices through which to detect, process, and solve various challenges [Halverson (2004)]. A safety strategy is thus not simply a written plan, but is actualized through practice. People learn to understand what *phronesis* is through practice, accomplished in dialogic interaction, and leading to organizational resilience.

6 CONCLUSION

The view from practice suggests that safety emerges out of interaction, dialogic sensemaking and collaboration, in which different 'parts' of the system learn with and from one another and take 'the other' into account in their own decisions and actions. This perspective recommends a dialogic approach that moves beyond the traditional dualism of 'top-down' and 'bottom-up' into a generative partnership between leadership and practitioners. An organizational design that embraces a dialogic approach and allows for emergence, creativity, and flexibility -- the cornerstones of collaborative work -- overcomes the limitations of 'top down' strategies that do not account for practice and leave the prevailing conditions within organizations unaddressed. Likewise, in contrast to 'bottom-up' initiatives that fail to connect on a systems level, a dialogic approach promotes system-wide organizational learning.

REFERENCES

Albolino, S., Cook, R., & O'Connor, M. (2007). Sensemaking, safety, and cooperative work in the intensive care unit. Cognition, Technology & Work, 9(3):131–137. doi: 10.1007/s10111-006-0057-5.

4 The collective property of a practice that is expressed in the open-ended set of doings and sayings [Schatzki (2002a)], « where people sense and dynamically negotiate their own and others goals, actions, expectations, needs and feelings » [Iedema2006b), p. 1112]

Antonsen, S. Safety culture and the issue of power. (2009). Safety Science, 47(2):183–191. doi: 10.1016/j.ssci.2008.02.004.

Bakhtin, M.M. (1981). The dialogic imagination: four essays. University of Texas Press, Austin.

Battles, J.B., Dixon, N.M., Borotkanics, R.J., Rabin-Fastmen, B., & Kaplan. H.S. Sensemaking of patient safety risks and hazards. (2006). *Health Services Research*, 41(4 Part II):1555–1575, 2006. doi: 10.1111/j.1475-6773.2006.00565.x.

Behara, R., Wears, R.L., Perry, S.J., Eisenberg, E., Murphy, L., Vanderhoef, M., Shapiro, M., Beach, C., Croskerry, P., & Cosby, K. (2005). *Advances in Patient Safety*, volume 2, A conceptual framework for studying the safety of transitions in emergency care, pages 309–321. Agency for Healthcare Research and Quality, Rockville, MD. URL http://www.ahrq.gov/downloads/pub/advances/vol2/behara.pdf.

Blackler, F., Crump, N., & McDonald, S. (2000). Organizing processes in complex activity networks. *Organization*, 7(2):277–300. doi: 10.1177/135050840072005.Boje, D.M. (2008). Storytelling organizations. Sage Publications, London.

Boreham, N.C., Shea, C.E., & Mackway-Jones, K. (2000). Clinical risk and collective competence in the hospital emergency department in the UK. *Social Science & Medicine*, 51(1):83–91. doi: 10.1016/S0277-9536(99)00441-4.

Bourdieu, P. (1977). Outline of a theory of practice. Cambridge University Press, Cambridge.

Bruner, J. (1991). The narrative construction of reality. *Critical Inquiry*, 18(1): 1–21. URL http://www.jstor.org/stable/1343711.

Callon, M. (1986). Some elements of a sociology of translation: domestication of the scallops and the fishermen of St. Brieuc Bay. In: Law J, editor. *Power, action and belief: a new sociology of knowledge*. London: Routledge and Kegan Paul; p. 196–223.

Cohen, M.D. & Hilligoss, P.B. (2010). The published literature on handoffs in hospitals: deficiencies identified in an extensive review. *Quality and Safety in Health Care*. 19(6): 493-497. doi: 10.11.36/qshc.2009.033480

Cohen, T., Blatter, B., Almeida, C., Shortliffe, E., & Patel, V. (2006). A cognitive blueprint of collaboration in context: Distributed cognition in the psychiatric emergency department. *Artificial Intelligence in Medicine*. 37(2):73–83. doi: 10.1016/j.artmed.2006.03.009.

Cook, R.I. & Rasmussen, J. (2005). "Going solid": a model of system dynamics and consequences for patient safety. *Quality and Safety in Health Care*. 14(2):130–134. doi: 10.1136/qshc.2003.009530.

Cook, R.I., Woods, D.D., & Miller, C. (1998). *A tale of two stories: Contrasting views of patient safety*. Chicago, IL: National Patient Safety Foundation.

Dekker, S.W.A. (2005). *Ten questions about human error: a new view of human factors and systems safety*. Mahwah, New Jersey: Lawrence Erlbaum Associates, Publishers.

Eden, C., Jones, S., Sims, D., & Smithin, T. (1981). The intersubjectivity of issues and issues of intersubjectivity. *Journal of Management Studies*. 18(1):37–47.
Engeström, Y. (1987). *Learning by expanding: an activity-theoretical approach to developmental research*. Helsinki: Orienta-Konsultit.

Fiske, S.T. & Taylor, S.E. (2008). *Social cognition: from brains to culture*. 3rd ed. Boston, MA: McGraw-Hill.
Foucault, M. (1980). *Power/knowledge: selected interviews & other writings 1972-1977*. Gordon C, editor. Toronto: Random House of Canada Limited.

Fox, S. (2000). Communities of practice, Foucault and Actor-Network Theory. *Journal of Management Studies*. 37(6):853–867. doi: 10.1111/1467-6486.00207.

Freire, P. (1993). *Pedagogy of the oppressed*. New York: Continuum; 1993.

Gherardi, S. & Nicolini, D. (2002). Learning in a constellation of interconnected practices: canon or dissonance. *Journal of Management Studies*. 39(4):419–436. doi: 10.1111/1467-6486.t01-1-00298.

Habermas, J. (1970). Towards a theory of communicative competence. *Inquiry: An Interdisciplinary Journal of Philosophy*. 13(1):360–375. doi:10.1080/00201747008601597.

Halverson, R. (2004). Accessing, documenting, and communicating practical wisdom: the phronesis of school leadership practice. *American Journal of Education*. 111(1):90–121. Available from: http://www.jstor.org/stable/3566883.

Herman, D. (2002). *Story logic: problems and possibilities of narrative*. Frontiers of narrative. Lincoln: University of Nebraska Press.

Hollnagel, E. (2009). The four cornerstones of resilience engineering. In: Nemeth CP, Hollnagel E, Dekker S, editors. *Preparation and Restoration*. No. 2 in Resilience Engineering Perspectives. Farnham: Ashgate; p. 117–133.

Hunte, G.S. (2010). Creating safety in an emergency department [dissertation]. University of British Columbia. Vancouver. Available from: https://circle.ubc.ca/handle/2429/27485.

Hutchins, E. (1995). How a cockpit remembers its speeds. *Cognitive Science*. 19(3):265–288. doi: 10.1016/0364-0213(95)90020-9.

Iedema, R., Flabouris, A., Grant, S., & Jorm, C. (2006a). Narrativizing errors of care: critical incident reporting in clinical practice. *Social Science & Medicine*. 62(1):134–144. doi: 10.1016/j.socscimed.2005.05.013.
Iedema, R., Rhodes, C., & Scheeres, H. (2006b). Surveillance, resistance, observance: exploring the teleo-affective volatility of workplace interaction. *Organization Studies*. 27(8):1111–1130. doi: 10.1177/0170840606064104.

Kirkeby, O.F. (2009). Phronesis as the sense of the event. *International Journal of Action Research*. 5(1):68–113. doi: 10.1688/1861-9916\ IJAR\ 2009\ 01\ Kirkeby.

Klein, G., Moon, B., & Hoffman, R.R. (2006a). Making sense of sensemaking 1: Alternative perspectives. *IEEE Intelligent Systems*. 21(4):70–73. doi:10.1109/MIS.2006.75.

Klein, G., Moon, B., & Hoffman, R.R. (2006b). Making sense of sensemaking 2: A macrocognitive model. *IEEE Intelligent Systems*. 21(5):88–94. doi: 10.1109/MIS.2006.100.

Latour, B. (1987). *Science in action: how to follow scientists and engineers through society*. Cambridge, MA: Harvard University Press.

Lave, J. & Wenger, E. (1991). *Situated learning: legitimate peripheral participation*. Cambridge: Cambridge University Press.

Law, J. (1986). Editor's introduction: power/knowledge and the dissolution of the sociology of knowledge. In: Law J, editor. *Power, action and belief: a new sociology of knowledge*. London: Routledge and Kegan Paul; p. 1–19.

Linell, P. (2009). *Rethinking language, mind, and world dialogically: interactional and contextual theories of human sense-making*. Advances in Cultural Psychology: Constructing Human Development. Charlotte, NC: Information Age Publishing, Inc. MacIntyre, A. (2007). *After virtue: a study in moral theory*. 3rd ed. Notre Dame, Indiana: University of Notre Dame Press.

March, J.G. (1991). Exploration and exploitation in Organizational Learning. *Organization Science*. 2(1):71–87. Available from: http://www.jstor.org/stable/2634940

Merleau-Ponty, M. (1962). *Phenomenology of perception*. London: Routledge.

McNiff, J. (2007). My story is my living educational theory. In: Clandinin DJ, editor. *Handbook of narrative inquiry: mapping a methodology*. Thousand Oaks, CA: Sage; p. 308–329.

Nöe, A. (2004). *Action in perception*. Cambridge, MA: MIT Press.

Nonaka, I. & Toyama, R. (2007). Strategic management as distributed practical wisdom (phronesis). *Industrial and Corporate Change*. June;p. dtm014. doi: 10.1093/icc/dtm014.

Patterson, E.S. & Wears, R.L. (2010). Patient handoffs: standardized and reliable measurement tools remain elusive. The *Joint Commission Journal on Quality and Patient Safety*. 36(2):52–61.

Perry, S.J. & Wears, R.L. (2009). Notes from underground: latent resilience in healthcare. In: Nemeth, C.P., Hollnagel, E. & Dekker, S., editors. *Preparation and restoration*. No. 2 in Resilience Engineering Perspectives. Farnham, Surrey: Ashgate; p. 167–178.

Rochlin, G.I. (2003). Safety as a social construct: The problem(atique) of agency. In: Summerton J, Berner B, editors. *Constructing risk and safety in technological practice*. London: Routledge. p. 123–139.

Rudolph, J.W. (2003). Into the big muddy and out again: Error persistence and crisis management in the operating room [Dissertation]. Boston College. Boston, MA.

Sanne, J.M. (2008). Incident reporting or storytelling? Competing schemes in a safety-critical and hazardous work setting. *Safety Science*. 46(8):1205–1222. doi: 10.1016/j.ssci.2007.06.024.

Schatzki, T. (2002). *The site of the social*. University Park, Pennsylvania: Pennsylvania State University Press.

Schubert, C.C. (2008) Healing the effects of medical errors: A vision of justice as wholeness. [dissertation]. Loma Linda University.

Schubert, C.C., Denmark, T.K., Crandall, B., Grome, A., & Pappas, J. (2013). Characterizing novice-expert differences in macrocognition: an exploratory study of cognitive work in the emergency department. *Annals of Emergency Medicine*. 61(1):96–109.

Suchman, L.A. (1987). *Plans and situated actions: the problem of human-machine communication*. Cambridge: Cambridge University Press.

Waring, J.J. (2009). Constructing and re-constructing narratives of patient safety. *Social Science & Medicine*. 69(12):1722–1731. doi: 10.1016/j.socscimed.2009.09.052.

Weick, K.E. (1995). *Sensemaking in organizations*. Thousand Oaks: Sage Publications.

Weick, K.E. & Roberts, K.H. (1993). Collective mind in organizations: heedful interrelating on flight decks. *Administrative Science Quarterly*. 38(3):357–381. Available from: http://www.jstor.org/stable/2393372.

Wells, G., O'Connor, C., Michaels, S. (2007). Semiotic mediation, dialogue and the construction of knowledge. Commentary. *Human Development*. 50(5):244–285.

Westrum, R. (1993). Cultures with requisite imaginations. In: Wise J, Hopkin V, Stager P, editors. *Verification and validation of complex systems: human factor issues*. Springer-Verlag; p. 401–416.

Woods DD. (2006). Resilience engineering: Redefining the culture of safety and risk management. HFES Bulletin. 49(12):1–3. Available from: http://www.hfes.org/web/BulletinPdf/1206bulletin.pdf.

Zack, M.H. (2000). Jazz improvisation and organizing: once more from the top. *Organization Science*. 11(2):227–234. Available from: http://www.jstor.org/stable/2640286. 9

EXPERIENCES FROM HEALTHCARE: - DESIGNING AND DEVELOPING ORGANISATIONS

SAFETY, ERROR, AND RESILIENCE: A META-NARRATIVE REVIEW

Robert L Wears [1] and Kathleen M Sutcliffe [2]
[1] University of Florida, Jacksonville, Florida, USA and Imperial College London, UK
[1] wears@ufl.edu, r.wears@imperial.ac.uk; +1 904 244 4508
[2] Johns Hopkins University, Baltimore, MD, USA
[2] ksutcli1@jhu.edu

Abstract

This paper analyses the development of safety in healthcare in three meta-narratives, each held by a different community of thought. The dominant narrative in healthcare is that of scientific-bureaucratic medicine, focusing on 'errors' as an objectively measured bit of external reality, best prevented by barriers, education, and exhoration – positively Safety-I. The second narrative is found in the safety sciences, which allow for more nuanced views, and at least to some extend hold developing capabilities to be equally as important as preventing 'errors' – moving at least in part to Safety-II. The third and least dominant of the narratives is that of patients and the public – a narrative of suffering and marginalisation – which sadly has shown little change over time. Brief contact between the health services and safety science communities in the mid to late 1990s set off the patient safety movement in the US and other countries. However, that contact was not sustained, and healthcare took away only a superficial and instrumental understanding, leading to a lack of progress.

1 INTRODUCTION

The focus on safety in healthcare is a relatively recent development, compared to that in other high hazard industries. Accordingly, studying the recent history and evolution of healthcare safety – how and why it came to be enacted in the way it did can highlight tensions and paradoxes common to safety (and performance) endeavours in general, by highlighting issues that may have slipped below the surface in more mature industries. This paper will provide a meta-narrative review of the rise and fall of healthcare safety.

2 META-NARRATIVE REVIEW

Meta-narrative review is an emerging analytic, synthetic method designed for topics that have been differently conceived of and studied by different epistemic communities. It was developed by Greenhalgh *et al* (2004; 2005), based loosely on Kuhn's notion of competition among scientific paradigms (Kuhn, 1970). Meta-narrative review focuses on how particular social concerns and research traditions related to an issue have unfolded over time, and how that evolution shapes the kinds of questions asked and the methods used to answer them. It also explores tensions and paradoxes among the various schools of thought, and in particularly how those tensions are exploited in power struggles.

2.1 Data Sources

Both formal and informal data sources were used to examine the history and evolution of healthcare safety. We primarily drew on written materials, in both the professional healthcare literature, the social science literature about healthcare, and the public press regarding safety. We also interviewed key participants in this evolution, and examined changes in speakers and topics over time.

2.2 Streams of Thinking and Narrative Voices

We identified 3 separate streams of thinking about safety and human performance in healthcare: a health services research stream advanced by what has been called 'scientific-bureaucratic medicine'; a narrative stream advanced by patients and families, largely in the public (*ie*, non-scientific) press; and a 'safety science' stream advanced by psychologists, engineers, and social scientists working on safety and performance in hazardous environments generally. We found Dekker's concept of 4 narrative voices – epistemological, preventive, moral, and existential – useful in illustrating how contradictions and paradoxes arise in these discourses (Sidney W. A. Dekker, 2014).

Health Service Research

Researchers in healthcare using typical epidemiological approaches had been studying adverse events since the 1950s (Barr, 1955). What is remarkable in this stream is that the 'objective' frequency of adverse events is roughly constant over the years – what changes however, is how that frequency was understood and interpreted (see

Table 1). This could be explained in two, non-mutually-exclusive ways. First, it could be that the perception of countable adverse events is a property of the measurement system / observer rather than the underlying reality. Second, it could be that the failure rate is constant, but the social understanding and acceptance of failures is changing, from a more tolerant to a less tolerant stance. It is ironic to note that exactly the same comparison to road traffic accidents was made in Illich's blistering critique (Illich, 1974) of healthcare published over 25 years earlier, for which he was roundly criticized for making an "ill-informed and irresponsible attack on the medical profession" (Bunker, 1997).

Table 0.1. Summary of the progressive evolution of safety thinking in healthcare

Source, datum	Interpretation	Appearances of 'error'
Barr (1955)	"the price we pay for medical progress"	Term never appears
Schimmel (1964) 20% adverse events, ~2% deaths	"the dangers of new methods must be accepted, and are generally warranted"	'error' specifically excluded
Mills (1977) ~5% adverse events, 1% major	"benefits and risks are inseparable … rates are remarkably low"	Term never appears
Steel (1981) 36% adverse events, 9% major, 2% deaths	Should seek to "reduce the number and severity"	Term never appears
Harvard Medical Practice Study (1991) 4% adverse events, ~1% deaths	"large and disturbing"	1st appearance of 'error' in only 1 of 4 papers from this study
Colorado / Utah / Institute of Medicine (2000) ~3% adverse events	Deaths exceed those from road traffic accidents	58 appearances of 'error' in Executive Summary alone

Safety Science

This history is well known to members of the resilience engineering community. In brief, safety science began in the late 19th century when industrial accidents, particularly railway accidents injured not only workers but innocent bystanders. It progressed from the idea of accident prone-ness in the 1920s (Burnham, 2009), to Heinrich's domino model in the 1930s. It began to be modified towards the end of World War II, when the concept of interaction between human and machine was added (Fitts & Jones, 1947). Major accidents such as Tenerife and Three Mile Island led to an efflorescence of activity in the 1990s (Woods, Dekker, Cook, Johannesen, & Sarter, 2010), since they were not satisfactorily explained by then prevailing notions. Much of the focus at this time was on figuring out exactly what was meant by 'human error' (Senders & Moray, 1991). It was at this point that health professionals made contact with the safety science community, and began to import at least some ideas (Lucian L. Leape, 1994). However, the safety world moved on from discussions of human error (at least in part) to more complex, emergent models of safety(Sidney W A Dekker, 2015; Hollnagel, 2014). Healthcare did not follow in this progression.

Patients and Public

The patient narrative is comprised of 'first stories' of suffering and loss. It generally uses the voices of boundary crossing, and existential suffering, and so frequently is at cross purposes with other discourses using epistemological or preventative voices. The litany of sufferers here is long, but celebrated cases include Libby Zion, Betsy Lehman, Willie King, Ben Kolb, Josie King, Jesica Santillan, Dennis Quaid, and Rory Staunton, to mention only a few. These stories have a disturbing sameness.

2.3 Mixing Streams and the Rise of Patient Safety

The fortuitous intermingling of these 3 streams in the mid 1990s set off the 'patient safety' movement in the US, UK, and other countries. In the US, legislation to reduce malpractice judgments were opposed by a litany of celebrated cases, and the effort was roundly defeated. Organized medicine needed to get on the right side of the safety issue, and so became a sponsor of the first Annenberg conference on healthcare safety in 1996. This brought the health service and patient narrative streams together. The health services and safety science streams met through the efforts of one of the authors of the Harvard study, who had framed the problem in terms of

'errors', and was guided to the burgeoning psychology, social science, and engineering literature on 'human erro' that followed TMI and other catastrophes.

At the same time, a technocratic managerial class was arising in healthcare, part of its delayed industrialization. The rhetoric of 'error' rather than risk or harm worked synergistically to advance this party by delegitimatizing the authority of the old authority of clinical expertise. Thus risk became 'error', and 'error' became a cause celebre, through a progressive reframing of risk that advanced the role of the new techno-bureaucratic managers, by employing a kind of 'folk psychology' of errors. Here we see how the tensions among the component narratives were exploited in contests for power and influence in the healthcare industry, and for control of the safety 'movement' in healthcare.

2.4 Separation and Fall of Patient Safety

Health professionals quickly grasped the relatively simple presentations of 'human error' published in their literature, and rapidly re-expressed them in medicalized language – not coincidentally keeping the new patient safety movement firmly under healthcare's control, and giving only lip service to partnership with the safety sciences.

3 DISCUSSION

Although resilience engineering does not wholly adopt the positivist approach common in many safety and quality circles, some users of the resilience language still often take concepts such as risk and safety as objective givens rather than as socially constructed, shared frames through which to view the world, at least as a first approximation. Although the paper will specifically focus on healthcare, this issues highlighted are increasingly relevant to other hazardous industries. In particular, there has been increasing interest in management circles in using healthcare as an exemplar for improving safety and human performance (Rousseau, 2006), as strange as that may seem, given that healthcare is a latecomer to the party. This seems more due to the psychological and organisational comfort afforded by the hubristic celebration of "evidence-based-ness" in medicine than to any real achievement in that field. Thus, lessons learned from the evolution of safety and performance understandings in healthcare may prove directly relevant to other domains, because those same desires for simple, certain answers that do not challenge those in power are common across all domains.

This analysis should advance our ability to create and sustain resilience by situating resilience thinking in a group of narratives that compete with it, helping to understand both opposition to resilience, and well-intentioned, instrumental misappropriation of it. In addition it will illustrate the role of power in creating a dominant narrative and the importance of plurality, and for maintaining a voice for neglected perspectives.

Acknowledgements

This work was supported in part by an Investigator's Award from the Robert Wood Johnson Foundation.

REFERENCES

Barr, D. P. (1955). Hazards of modern diagnosis and therapy -- the price we pay. *JAMA: The Journal of the American Medical Association, 159*, 1452 - 1456.

Bunker, J. P. (1997). Ivan Illich and the pursuit of health. *J Health Serv Res Policy, 2*(1), 56-59.

Burnham, J. C. (2009). *Accident Prone*. Chicago, IL: University of Chicago Press.

Dekker, S. W. A. (2014). The psychology of accident investigation: epistemological, preventive, moral and existential meaning-making. *Theoretical Issues in Ergonomics Science, on line ahead of print*, 1-12. doi: 10.1080/1463922X.2014.955554

Dekker, S. W. A. (2015). *Safety Differently: Human Factors for a New Era*. Boca Raton, FL: CRC Press.

Fitts, P. H., & Jones, R. E. (1947). *Analysis of factors contributing to 460 'pilot error' experiences in operating aircraft controls*. Air Material Command, Wright-Patterson Air Force Base. Dayton, OH. Retrieved, from

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of Innovations in Service Organizations: Systematic Review and Recommendations. *Milbank Quarterly, 82*(4), 581-629. doi: 10.1111/j.0887-378X.2004.00325.x

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., Kyriakidou, O., & Peacock, R. (2005). Storylines of research in diffusion of innovation: a meta-narrative approach to systematic review. *Soc Sci Med, 61*(2), 417-430. doi: 10.1016/j.socscimed.2004.12.001

Hollnagel, E. (2014). *Safety-I and Safety-II: The Past and Future of Safety Management*. Farnham, UK: Ashgate.

Illich, I. (1974). Medical Nemesis. *Lancet, 303*(7863), 918-921. doi: doi:10.1016/S0140-6736(74)90361-4

Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (2000). *To Err Is Human - Building A safer Health System*. Washington, D.C.: National Academy Press.

Kuhn, T. S. (1970). *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.

Leape, L. L. (1994). Error in medicine. *Journal of the American Medical Association, 272*(23), 1851-1857.

Leape, L. L., Brennan, T. A., Laird, N., Lawthers, A. G., Localio, A. R., Barnes, B. A., Hebert, L.*, et al.* (1991). The nature of adverse events in hospitalized patients. Results of the Harvard Medical Practice Study II. *N Engl J Med, 324*(6), 377-384.

Mills, D. H., Boyden, J. S., & Rubamen, D. S. (Eds.). (1977). *Report on the Medical Insurance Study*. San Francisco, CA: Sutter Publications.

Rousseau, D. M. (2006). 2005 Presidential Address: Is There Such a Thing as "Evidence-Based Management"? *The Academy of Management Review, 31*(2), 256-269. doi: 10.2307/20159200

Schimmel, E. M. (1964). The Hazards of Hospitalization. *Ann Intern Med, 60*, 100-110.

Senders, J. W., & Moray, N. P. (1991). *Human Error: Cause, Prediction, and Reduction*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Steel, K., Gertman, P. M., Crescenzi, C., & Anderson, J. (1981). Iatrogenic illness on a general medical service at a university hospital. [Research Support, U.S. Gov't, P.H.S.]. *N Engl J Med, 304*(11), 638-642. doi: 10.1056/NEJM198103123041104

Thomas, E. J., Studdert, D. M., Burstin, H. R., Orav, E. J., Zeena, T., Williams, E. J., Howard, K. M.*, et al.* (2000). Incidence and types of adverse events and negligent care in Utah and Colorado. *Medical Care, 38*(3), 261-271.

Woods, D. D., Dekker, S. W. A., Cook, R. I., Johannesen, L., & Sarter, N. (2010). *Behind Human Error* (2nd ed.). Farnham, UK: Ashgate.

WHAT CAN NON-ROUTINE EVENTS (NRES) TEACH US ABOUT MANAGING RESILIENCE?

Renaldo C. Blocker, Ph.D. [1]
[1] Department of Health Sciences Research, Mayo Clinic, Rochester, MN, USA
[1] blocker.renaldo@mayo.edu

Abstract

Introduction: Non-routine events (NREs) are a source of potential harm to the safety of patients since NREs represent disruptions in everyday clinical activities or processes that are otherwise conducted seamlessly. NREs are defined as "any event that is perceived by care providers or skilled observers to be distracting, undesirable, unusual, or atypical" (Schraagen, 2011; Weinger & Slagle, 2002). NREs can be both positive and negative, but researchers typically focus on the negative aspect in order to examine ways to decrease the likelihood of NREs leading to a medical error. Prospectively capturing NREs provides a mechanism for examining the resilience in a system. Comprehensive NREs studies are essential to understanding NREs intrinsic ability to impact health care processes and outcomes. Understanding NREs impacts on a system and/or team can help with learning and understanding how a system adjust its functioning during expected and unexpected conditions (Hollnagel et al., 2011). Therefore, the present study prospectively examined the characteristics of NREs and their impacts on the surgical team during cardiac surgery.

Method: This was a post-hoc analysis of a prospectively collected dataset obtained through direct, targeted observations using an electronic data collection tool (Blocker et al., 2010). The electronic data collection tool captured the description of the NREs, the surgical phase that the NREs occurred, the potential and/or actual impact of the NREs, and the surgical team members involved in the NREs. The observation team collected data over a 6 month period in multiple operating rooms within two midwestern hospitals and across multiple surgical teams. Convenience sampling was used to select the hospitals and the cardiac surgical cases to observe (Malterud, 2001). Descriptive statistics were primarily used to analyze the characteristics of NREs during the cardiac surgical procedures. As implied for this particular research study, the dependent variable is the NREs and the independent variables are cardiac surgical procedures at the two nonprofit academic hospitals.

Results: Across all 36 observed cardiac surgical cases, on average there were 56.55 non- routine events per case (SD = 29.262; range: 14 –122). The majority of the non-routine events were environment related (52.55%) followed by technology related non-routine events (13.51%). Non-routine events occurred during all the surgical phases, but most frequently in surgical repair (30.35%), opening (23.77%) and induction (15.62%). A large portion of the non-routine events involved the nurse and surgeon (43.86%). However, the non-routine events typically were considered as having a momentary distractions impact, meaning that there was a brief pause in the flow of the operation that lasted more than 10 seconds. There were no significant differences in NREs frequency, type and impact between the two hospitals.

Discussion: Capturing NREs and examining the characteristics of NREs can provide us with a mechanism for examining our ability to respond to events and to learn from past failures and success, which are important cornerstone of resilience engineering (Hollnagel et al., 2011). The results provides us with knowledge for creating resilience in a system. The characteristics of NREs captured in this study helps us with learning (knowing what has happened), responding (knowing what to do), monitoring (knowing what to look for) and anticipating (knowing what to expect). The results suggest that NREs impacts the surgical team function and knowing how to respond, anticipate and monitor them is critical in reducing distraction-induced errors.

REFERENCES

Blocker, R.C., Eggman, A., Zemple, R., Wu, C.E., & Wiegmann, D.A. (2010). Developing an observational tool for reliably identifying work system factors in the operating room that impact cardiac surgical care. *Human Factors and Ergonomics Society Annual Meeting Proceedings, Health Care, 5,* 879-883.

Hollnagel, E., Paries, J., Woods, D., and Wreathall, J. (2011). Resilience Engineering in Practice: A Guidebook. England, UK: Ashgate Publishing Limited.

Malterud, K. (2001). Qualitative research: Standards, challenges and guidelines. *The Lancet, 358,* 483-488.

Weinger, M.E. & Slagle, J. (2002). Human factors research in anesthesia patient safety: Techniques to elucidate factors affecting clinical task performance and decision making. *Journal of the American Medical Informatics Association,* 9(6), S58-S63.

Schraagen, J.M., Schouten, T., Smit, M., Hass, F., Beek, D., Ven, J., Barach, P. (2011).

A prospective study of paediatric cardiac surgical Microsystems: Assessing the relationships between non-routine events, teamwork and patient outcomes. *British Medical Journal Quality & Safety, 20(7)*, 599-603.

TOWARDS A RESILIENT AND LEAN HEALTHCARE

Tarcisio Abreu Saurin[1] and Jeanette Hounsgaard[2]
[1]Federal University of Rio Grande do Sul, Av. Osvaldo Aranha 99, 5. andar, CEP 90035-190, Porto Alegre, RS, Brazil
[1]saurin@ufrgs.br; Tel: +55-51-9628-2554
[2]Centre of Quality, P. V. Tuxensvej, 5500 Middelfart, Denmark
[2] jeanette.hounsgaard@rsyd.dk

Abstract

Although lean production is mostly known for its applications in the manufacturing industry, it has increasingly spread to a number of other sectors, including the so-called complex socio-technical systems (CSSs), such as healthcare. In fact, a number of lean principles and practices are in line with the premises of resilience engineering (RE) and complexity theory, such as the encouragement for understanding work-as-done and giving visibility to processes and outcomes. Some possible conflicting areas between both paradigms also exist, since lean is mostly focused on increasing efficiency while RE usually stresses safety. In particular, ill-thought- out lean implementations can disregard the value of slack as a resource for dealing with unexpected situations that are typical of CSSs. This drawback may be due to both the lack of an assessment of the wider impacts of lean interventions as well as a narrow view of what counts as slack – indeed, slack may take many forms, such as time, materials, redundant equipment, and cognitive diversity. Therefore, lean and RE have practical and theoretical relevance to each other, and due to this fact the proposed workshop aims at the discussion of synergies and pitfalls of using both together, emphasizing the context of healthcare.

In principle, it is suggested a 2-hour workshop, involving: (i) an introductory 10 minute presentation addressing the main relationships between lean and RE; (ii) two 15 minute presentations concerned with the use of the Functional Resonance Analysis Method (FRAM) for assessing the solutions proposed by lean in hospitals in Brazil and Denmark – these presentations will be made by the organizers of the workshop, and one of them was submitted as a book chapter for the upcoming new book of the Resilient Health Care Network (please see this chapter attached to the present submission); (iii) presentations of regular papers submitted to the conference and linked with the topic of the workshop; and (iv) discussion and identification of opportunities for research and collaboration. The minutes of the workshop will be recorded and sent to all participants after the symposium.

COMMUNITY RESILIENCE

A PARTICIPATORY APPROACH TO IMPROVE RESILIENCE IN COMMAND AND CONTROL (C2) SYSTEMS: A CASE STUDY IN THE RIO DE JANEIRO C2 SYSTEM

Paulo Victor R. de Carvalho [1] , Diana Arce[2], Claudio Passos[2], Gilbert J. Huber[2], Marcos Borges[2] and José Orlando Gomes [2]
[1] Instituto de Engenharia Nuclear, Rua Hélio de Almeida 75, Rio de Janeiro, Brasil
[1] paulov195617@gmail.com tel.: +5521995048527
[2] UFRJ, Cidade Universitária, Rio de Janeiro, Brasil
[2] joseorlando@nde.ufrj.br

Abstract
A fundamental Command and Control Centre (C2) strategy is to forecast and plan responses to incidents. However, there are incidents that defy forecasting and/or planning, cannot be completely understood while they're occurring, and should be treated ad-hoc. Such incidents, if not properly managed, may produce catastrophic outcomes. This article describes how the Integrated Command and Control Centre of Rio de Janeiro City (CICC-RJ) responded to unexpected and improbable events related to protests that took place during the 2013 FIFA Confederations' Cup in Rio de Janeiro.

Keywords: C2 Center, protests, unexpected, Rio de Janeiro, Resilience

1. INTRODUCTION

Rio de Janeiro State has an Integrated Command and Control Center (locally referred to as CICC-RJ) based on C2 Model (Builder, Bankes and Nordin, 1999) that seeks to promote coordination among security, health, transportation and public service agencies by providing a venue for their interaction. These agencies deal with routine daily operations, emergencies, large events (e.g. major weather events), and Large Events (e.g. FIFA World Cup).

At the time of the events considered in this article, CICC-RJ was grappling with challenges on three fronts: it had a Large Event (FIFA Confederations Cup) under way; it was undergoing tests for FIFA's World Cup competition (which included the Confederations Cup); it and its participating agencies were learning to interoperate. In the midst of this, unexpected massive protest demonstrations arose, driving the Centre's operations beyond previously considered bounds.

The aim of this paper is to analyze, through a scientific perspective, how the CICC-RJ behaved face of the unknown and discuss aspects of resilience and brittleness of the organization against these incidents. To do this we used several techniques of Cognitive Task Analysis (CTA) (Crandall, Klein and Hoffman, 2006) to better understand people's work at the CICC-RJ.

2 CICC-RJ ORGANIZATION, STRUCTURE, AND OPERATION

Rio de Janeiro State's Integrated Command and Control Centre is one of six similar regional nodes in Brazil's National Integrated Command and Control System (SICC). As a regional node of SICC it coordinates neighbouring states' CICCs when appropriate. In its usual role as the state's CICC it provides a common organizational structure to enable local public service organizations to work collaboratively. It can deploy mobile units that are adapted trucks that aim to provide tactical support and are equipped with communications, video monitoring, and event management systems.

CICC-RJ coordination ensures the smooth running of the Centre and promotes the integration of the participating organizations. Each of the participating organizations retains its autonomy and command structure, and shares, or not, its information and experiences with other agencies. At the time of the FIFA Confederations Cup and the events reported here the participating organizations were just beginning to be integrated into the Centre.

Communication between agencies happens through each agency's representative, in person. Although each agency has a phone available for internal and external communication, interviewees reported and observations corroborate that these phones are hardly ever used for interagency communication.

The CICC does not impose a communication standard upon participating agencies. Agencies use their own pre-existing means (often radio) for intra-agency communications, augmented *ad hoc* by instant messaging or chat software apps, not provided by the Centre.

2.1 FIFA Confederations Cup 2013 plan

During the Confederations Cup, the CICC-RJ housed the following agencies:

- **Security**: Federal Police (PF), Federal Road Police (PRF), National Security Force (FSN), Air Defense Command and Control (CCDA), Cyber Defense Centre (CDCIBER), Military Police (PMERJ), Civil Police (PCERJ), Municipal Guard (GM-Rio)
- **Safety**: Civil Defense, Mobile Emergency Service (SAMU), Fire Department (CBMERJ)
- **Transportation**: Highway concessionaire (Lamsa), Train Company (Supervia), Traffic Engineering Co. (CET-RIO), Urban Transportation Office (SMTU), Bridge Concessionaire (CCR / Ponte), Airport Infrastructure Co. (INFRAERO), Transport Agency (Agetransp), Subway Company (MetroRio)
- **Communication**: Telecommunication Agency (Anatel).
- **Public Administration**: Operations' Centre of Rio de Janeiro City (COR - RIO), Rio de Janeiro State Chief of Staff, Internal Revenue Service (RF), FIFA Local Organizing Committee (COL).

CICC-RJ's Confederations Cup plan mapped out in detail the competition's areas of interest. These included stadiums, hotels where the national teams, referees and FIFA representatives were staying, the routes between those hotels and other areas of interest and other events related to the Confederations Cup. The plan also mapped out other events of interest which, although not directly related to the Confederations Cup, involved the presence of someone related to the Cup (e.g. players' visits to slums, parties, and so on). Every item listed received an action plan aimed to prevent incidents and protect the public directly and indirectly involved in the Confederations Cup. These action plans involved: escort of delegations, blocking streets near Maracanã Stadium, police reinforcements, mass transportation services, unauthorized radio broadcast monitoring, strategic positioning of the police and public safety agents, intense monitoring by cameras throughout the city, telemetric systems, georeferencing, firearms detection systems, among others.

3 RESEARCH METHODOLOGY

Cognitive Task Analysis (CTA) techniques were employed to understand and study the process of managing major events (Crandall, Klein and Hoffman, 2006) to identify and analyse aspects of CICC-RJ resilience and brittleness. The research team chose the CTA because this is a study applied to a complex context where events happen in a nonlinear manner and need a systemic approach to be analysed (Hollnagel, 2006). The research comprises two steps: data collecting, and analysis and representation.

The CTA techniques used were:

1. to capsulize incident accounts to reduce the interviews' observations' narratives, and to capture key decisions, using key words such as: protest, planning, coordination, cooperation, communication, areas and events of interest, transportation, incident, and emergency, among others.
2. to use criteria for grouping cues, actions, and patterns culled from the database and interviews to generate a critical cue inventory. The criteria adopted were: incident solving, inter-agency collaboration, intra-agency communication (between representatives at CICC and agents in the field), and conflict resolution
3. to search for and identify a set of themes to provide a convenient view of the flow of activities through time. The themes we adopted are listed below:

    - **Planned Events** – items such as games, road blocks and detours, mobilization of security officers, escorting teams, referees, FIFA and government representatives, etc. Source: CICC-RJ database.
    - **Realized Events** – record of performed actions, planned or otherwise. Sources: CICC-RJ database and interviewees.
    - **Unexpected Events** – incidents directly related to the protests that occurred on the day of the game. Sources: CICC-RJ database and interviewees.
    - **Information Requests** – information requests between the CICC-RJ and field agents during the protest. Source: Interviewees.
    - **Decisions** – key decisions made toward ending the protest, by personnel at the CICC-RJ or field agents. Source: Interviewees.
    - **Feedback** – field agent reports to the CICC-RJ on effects of decisions. Source: Interviewees.
    - **Other Incidents** – incidents not directly related to the protests, such as illegal ticket sales, robberies, etc. Source: CICC-RJ database.

4 DATA ANALYSIS AND REPRESENTATION

We used a timeline with swim-lanes to represent the elicited data. The timeline shows events in Rio de Janeiro on June 16th, 2013, day of the Italy vs. Mexico game. It represents the sequence and duration of events, incidents, actions, perceptions and decisions. It attempts to show the communication among the various agencies involved in the events and how the decision making process actually transpired. Figure 2 is a sample that illustrates several events spanning a little more than an hour of that day.

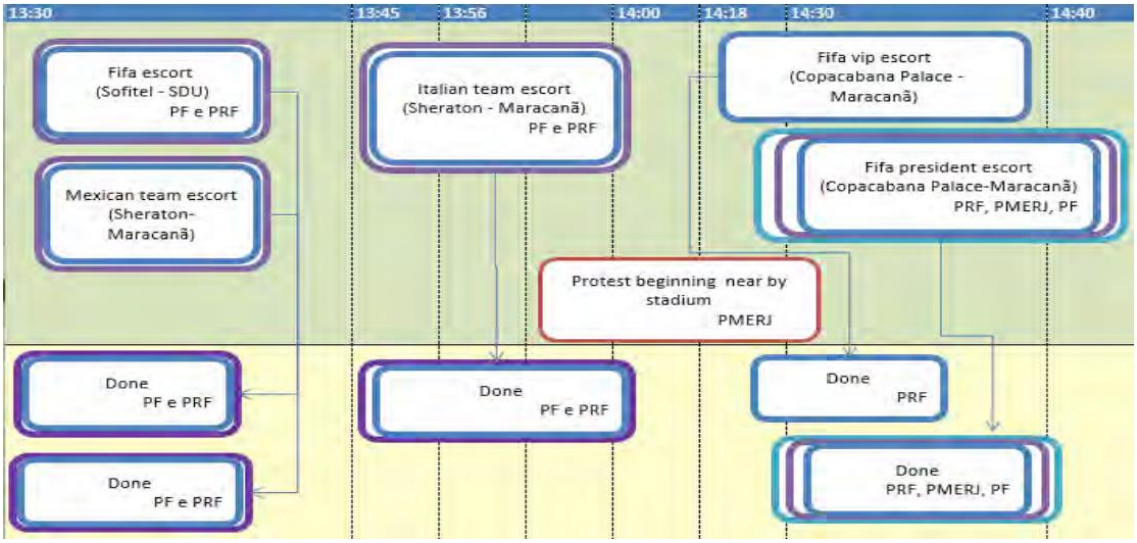


Figure 1. Timeline, June 16th 2013, 1:30pm to 2:40pm

The records and timeline show actions by 11 of the 24 CICC-RJ participating agencies:

- **Security**: Federal Police (PF), Federal Road Police (PRF), National Security Force (FSN), Military Police (PMERJ), Civil Police (PCERJ)
- **Safety**: Fire Department (CBMERJ)
- **Transportation**: Bridge Concessionaire (CCR / Ponte), Transport Agency (Agetransp), Subway Company (MetroRio)
- **Communication**: Telecommunication Agency (Anatel).
- **Public Administration**: FIFA Local Organizing Committee (COL).

The juxtaposition of planned and realized events on the timeline highlights the discrepancies between actions as planned and as realized, due to plan input issues (e.g. updates to personnel movement), execution issues, and changes in circumstances (e.g. demonstrating crowds). Two striking absences were reported in the interviews and visible in the database: plan changes and under-reporting of realized actions. Plan change information input into the database overwrote planned events records, leaving no change history and making it impossible to assess plan evolution dynamics, and the change's possible impact on execution. We checked other Confederations Cup game days for under-reporting of realized actions, and observed this to be a broad pattern. These absences are unfortunate, as they undermine the CICC-RJ's organizational learning and ability to improve its planning and operations.

4.1 The Protest

During the pre-game mobilization, Military Police in the field perceived people gathering, and at approximately 2pm alerted the CICC-RJ that a protest demonstration was forming. The leadership at the CICC-RJ decided to not interfere in the developments at that time, but to maintain a watch on the unfolding activity. Officers on patrol in the field detected people carrying potentially dangerous materials and apprehended gasoline and opportunity weapons such as rocks and wood planks. At 3pm the protesters moved to occupy the streets near Maracanã Stadium. The game was scheduled to start at 4pm. The officer in charge of the Military Police troops in the field decided to intervene and preclude that the protesting demonstrators reach the Stadium. The ensuing mayhem resulted in injuries, tear gas intoxication, property depredation, and arrests.

In their effort to keep the protesters from reaching Maracanã Stadium, the military police drove them towards the Quinta D'Or Hospital. Panic broke out and people sought shelter in the hospital, whose entrance was

vandalised. From the vicinity of the hospital the protesters were driven to Ceará St., from where the demonstrators dispersed around 7pm. Details of these actions were not recorded in the CICC-RJ database.

4.2 Few Collaborative Actions

Analysis of the available data on this protest incident indicates a low level of collaboration among the participating agencies and a low level of interaction between officers at the CICC-RJ and in the field. Only 2 of the 25 actions represented on the timeline to manage incidents were collaborative. The officer in the field made most decisions alone: of the 19 communications actions related to this incident identified by this study only 7 were between field agents and the CICC-RJ.

The interviewees reported that not enough information flowed from the field to support decision making at the CICC-RJ. Examples of information they would have liked to see in the studied incident included whether weapons were present (how many and which type); protest leadership; presence of people with limited capability (children, elderly, handicapped, etc.); if the movement towards the train and subway stations was in search of refuge or a protest action; if there were injured people; etc. This information would have been useful to support decisions on whether to keep stations open or close them, and on whether to mobilize more police or paramedics to the protest site.

4.3 Supportive infrastructure

CICC-RJ is the first time working together in a single location for many of its participating agencies. The building that houses it has easy access, "intelligent", with well distributed and accessible spaces. It is use-oriented and an example of space designed to enhance the resilience of the institution (Botterell and Griss, 2012). Agency representatives were trained in the use of the space and technology available in the Command and Control Centre.

It was observed that these agencies work together in planning and implementing activities related to major events. Also that CICC-RJ has norms that aim to structure the organization and resolve doubts about planning, areas of activity and limits of each agency, the operationalization of the system, etc. How people actually perform their work (normal behaviour) usually differs from procedures (normative behaviour). This dichotomy was observed when the unexpected protests broke out. At that moment the crisis response plan's inadequacies led agencies' representatives at CICC-RJ to work in an a*d hoc* mode (improvisation), without a clearly defined structure for decision making. While this was reported as an unwelcome surprise by the interviewees, the distinction between normal (realized) and normative (prescribed) behaviours is not unusual (Hollnagel, 2006; Gomes et al., 2009). The difference between normal and normative behaviours does not necessarily cause a failure (Dekker, 2006); much to the contrary, it may strengthen coupling.

4.4 Communication

Interviews and observations showed that communications between the field and the CICC-RJ suffered from lack of structure and resources. Field personnel used radio and mobile phones to report any relevant information to their respective agencies at the CICC, who then proceeded to disseminate it verbally among the other agencies present. The absence of an established information sharing structure compromised the CICC's and agencies' situational awareness, and impaired their ability to respond promptly and appropriately.

Near game-time on June 16th, near the stadium, the challenge was to make best use of the forces present to keep the flow of game-goers moving and separate from demonstrators, and to isolate the small number of violent demonstrators ('black-blocks') from the larger mass of peaceful ones. Achieving this while attempting to maintain the CICC informed using the existing communications resources revealed the extreme workload involved, and most decisions were made with little CICC interaction. To get some level of situational awareness, CICC agents resorted to local TV news, Internet 'Ninja' Media raw reports, and monitoring cameras.

4.4 Poor Preparedness

CICC-RJ preparedness is poor due to several factors:

1. Absences: agencies are not required to participate in the CICC-RJ, and some don't.
2. Lack of continuity: agency representatives participating in planning meetings aren't necessarily the ones tasked with execution, inexistent handover design.
3. Poor simulation exercises: although simulation exercises were undertaken, they suffered from low fidelity (policemen cast in the role of rioters [were apathetic | played the part unconvincingly]) and incompleteness (health and transportation agencies were absent; geography was not covered).

4. Untrained personnel: CICC-RJ management provided training in its processes and technologies to all participants, but agency personnel changes undermined this, compromising collective performance.

5 CONCLUSION

This study sought to understand the operation of a C2 centre, how it worked on the preparation and execution of safety and security actions of a major sporting event, and how it dealt with unexpected violent protests that broke out during the event. The planning for the Confederations Cup of the studied centre was successful since the escort, scheduled events and games happened as expected. There was no need to deploy alternative plans, but improvisation played a key role in achieving satisfactory results.

We believe that there is still much work ahead especially in relation to crisis management. Although participants of the agencies had some understanding of their roles and executed some joint actions, what was observed was lack of efficient communications and coordination between agencies, and poor decision making processes. The CICC-RJ should review and update its infra-structure and organization design to improve these issues, and others, related to knowledge management, that are compromising its preparedness, such as handover, debriefing, and lesson learning. Its preparedness must be improved through higher fidelity simulation exercises.

In our view, it is extremely important to develop systems capable of capturing the unfolding of events and supporting the execution of actions; supporting tactical and operational decision making; capturing incidents and supporting the deployment of resources to solve these incidents; and supporting communication. These systems should maintain records of all activity, including communication recordings, for use in possible studies and improvement plans. Additionally, these systems should be designed to support not one, but a variety of Command and Control approaches and, as a result, be better able to cope with unexpected communications and interoperability challenges even during stress situations.

As future work this research team will propose the construction of the aforementioned systems and will continue to analyse the CICC-RJ's operations, both run-of-the-mill and the exceptional ones, be these emergent large events or scheduled Large Events, such as the upcoming Olympic Games in 2016. The purpose of the analysis is to propose, in collaboration with members of the CICC-RJ, techniques, frameworks, software and processes that are able to increase the resilience of this centre.

REFERENCES

BBC. (2013) Blogueiros revelam várias caras e causas de protestos, Retrieved from http://www.bbc.co.uk/portuguese/noticias/2013/06/130626_palanque_novo_protestos_bg.shtml.

Botterell, A. and Griss, M. (2012) A Pragmatic Approach to Smart Workspaces for Crisis Management, *Proceedings of the 9th International ISCRAM Conference*.

Builder, C. H., Bankes, S. C. and Nordin, R. (1999) Command Concepts: A theory derived from practice of command and control, RAND, Santa Monica, CA.

Calderon, A., Johnson, P. and Hinds, J. (2013) Leading Cats: How to Effectively Command Collectives, *Proceedings of ISCRAM 2013*, 32–41.

Crandall B., Klein G. and Hoffman R. (2006) Working minds: a practioners guide to cognitive task analysis, MIT Press, Cambridge.

Dekker, S. (2006) Resilience Engineering: Chronicling the Emergence of Confused Consensus, In: Resilience Engineering: Concepts and Precepts, Ashgate, London, UK, 68 – 83.

Estadão. (2013) Onda de protestos no País já tem seis mortes, available in O Estadão: http://www.estadao.com.br/noticias/cidades,onda-de-protestos-no-pais-ja-tem-seis-mortes,1047624,0.htm 13. G1. (2013) A Linha do tempo das Manifestações, avaiable in G1: http://g1.globo.com/brasil/linha-tempo-manifestacoes-2013/platb.

Globo. (2013) Manifestantes que estavam acampados no Leblon são recebidos por Cabral e pedem mais segurança, available in O Globo: http://oglobo.globo.com/rio/manifestantes-que-estavam-acampados-noleblon- sao-recebidos-por-cabral-pedem-mais-seguranca-8831612.

Gomes J. O., Woods D., Carvalho P. V. and Huber, G. J. and Borges M. (2009) Resilience and brittleness in the off shore helicopter transportation system: The identification of constraints and sacrifice decisions in pilots' work. *Reliability Engineering & System Safety*, 94(2), 311-319.

Grant, T., Geugis, F., Jongejan, P., (2013) Social Media in Command & Control: A proof-of principle experiment, *Proceedings of ISCRAM* 2013. 52 - 61.

Hamilton, J.A., Melear J. and Endicott, G. (2002) C2 Interoperability: Simulation, Architecture and Information Security, *Proceedings of the 7th International Command and Control Research and Technology Symposium.*

Hoffman, R., Crandall, B. and Shadbolt, N. (1998) Use of the critical decision method to elicit expert knowledge: A case study in the methodology of cognitive task analysis, *Human Factors: The Journal of the Human Factors and Ergonomics Society 40.2*, 254-276.

Hollnagel, E. (2006) Resilience – the Challenge of the Unstable, In: Resilience Engineering: Concepts and Precepts, Ashgate, London, UK, 8 – 17.

Lanfranchi V., Mazumdar S. and Ciravegna F. (2013) Evaluating the real usability of a C2 system – short and controlled vs long and real. *Proceedings of ISCRAM 2013*, 62 - 66.

Paggoto, J. and O'Donnell, D. (2012) Canada's Multi-Agency Situational Awareness System – Keeping it Simple, *Proceedings of ISCRAM 2012*, 1 - 10.

Woods, D. (2006) Essential Characteristics of Resilience. In: Resilience Engineering: Concepts and Precepts, Ashgate, London, UK, 18 – 30.

MULTIOBJECTIVE FORMULATION FOR NETWORK RESILIENCE: A TRADE-OFF BETWEEN VULNERABILITY AND RECOVERABILITY

Kash Barker[1], Nazanin Morshedlou[2], Jose E. Ramirez-Marquez[3]
[1] University of Oklahoma, School of Industrial and Systems Engineering, Norman, OK, USA
[1] kashbarker@ou.edu, 405.325.3721
[2] University of Oklahoma, School of Industrial and Systems Engineering, Norman, OK, USA
[2] nazanin.tajik@ou.edu
http://www.ou.edu/systemslab
[3] Stevens Institute of Technology, School of Systems and Enterprises, Hoboken, NJ, USA
[3] jmarquez@stevens.edu

Abstract.
The ubiquitous nature of infrastructure networks in today's society makes them a particularly important focus of preparedness planning, as their operation is essential for the many socioeconomic functions that rely upon them. Apart from that, many global disasters have prompted the need to study and plan for resilience. Despite previous work, which focus on after disruption partially, the work proposed here provides an initial multi-objective mathematical programming formulation based on reliability, vulnerability, and recoverability of the system to strengthen network resilience by emphasizing vulnerability and recoverability. The trade-off of investments made in both mitigation (vulnerability) and contingency (recoverability). Experimental results for both deterministic and stochastic conditions are presented, demonstrating the effectiveness and efficiency of the proposed model.

1 INTRODUCTION

The ubiquitous nature of infrastructure networks in today's society makes them a particularly important focus of preparedness planning, as their operation is essential for the many socioeconomic functions that rely upon them. No longer is it sufficient to focus on "prevention and protection" from the inevitability of disruptive events, potentially large-scale in nature. Recent natural disasters (e.g., hurricanes, earthquakes) have demonstrated an ability to overwhelm infrastructure networks regardless of the levels of prevention and protection. According the US National Academies of Science [2012], "One way to reduce the impacts of disasters on the nation and its communities is to invest in enhancing resilience […]."

The US government, through several agencies including the Department of Homeland Security (DHS), has increasingly emphasized resilience planning for critical infrastructure. Presidential Policy Directive 21 [Obama 2013] states that critical infrastructure "must be secure and able to withstand and rapidly recover from all hazards," where the combination of "withstanding" and "recovering" from disruptions constitutes resilience. *Resilience* has increasingly been seen in the literature [Hosseini et al. 2015, Park et al. 2013, Zolli and Healy 2012]. Ramirez-Marquez and co-authors offer a paradigm for system performance following a disruption, shown in Figure 1 [Henry and Ramirez-Marquez 2012, Barker et al. 2013, Pant et al. 2014, Baroud et al. 2014]. Network performance is quantified by a general performance measure □(□) (e.g., traffic flow or delay for a highway network). System resilience at time *t* is exhibited after a disruption, □□, which affects the original system state. Based on this description, system resilience has been defined as a time-dependent and disruption-specific ratio $\text{Recovery}(\square)/\text{Loss}(\square_d)$.

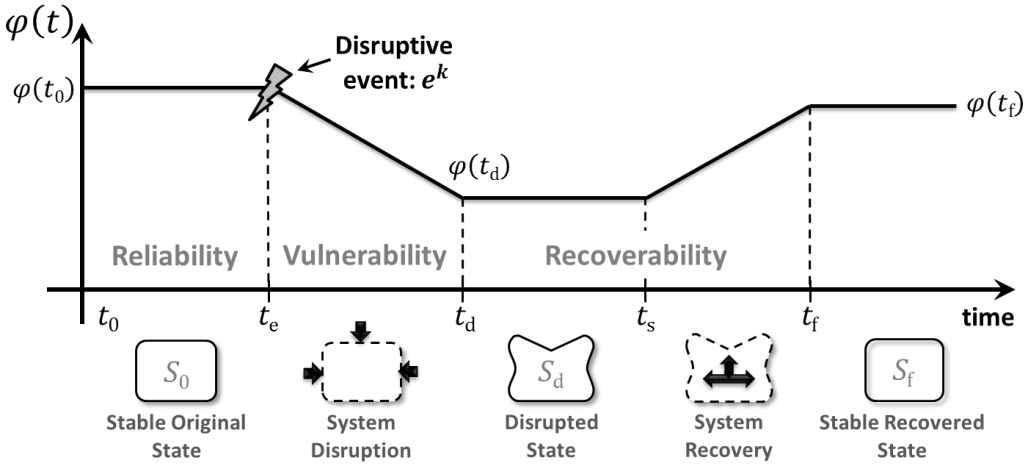


Figure 1. System performance across system states.

Figure 1 highlights two primary dimensions that resilient systems exhibit after a disruptive event: vulnerability, or an inability to maintain a desired performance level after a disruption, and recoverability, or an ability to recover timely.

This paper addresses a multi-objective mathematical model for resilient networks which simultaneously considers (i) network vulnerability by reducing the impact initially experienced after a disruption, and (ii) network recoverability by finding the most effective ordering of the restoration of disrupted links.

The aim of this paper is to introduce an initial multiobjective mathematical model which (i) considers the proportional disruption in links, (ii) minimizes the vulnerability of network by assigning resources in presence of disaster, (iii) minimize the cost of unsatisfied demand (e.g. in transportation networks, the amount of traffic unable to reach a destination, or in electric power networks, the amount of electricity unable to be delivered from supplier nodes to customer nodes), (iv) minimizes the time of recovery by finding the best order of link to be recovered, (v) balances between the investments on vulnerability reduction and recoverability enhancement, and (vi) accounts for uncertainty in parameters of the formulation with stochastic optimization methods.

2 BRIEF BACKGROUND

Among the recent literature regarding network disruption and restoration, Lee and Wallace (2007) consider the importance of interdependent infrastructures, an example of five infrastructure such as communication, transportation, and power grids, in a network flow and represent a mathematical model to guide the system to restore after a disaster. The first attempts of resource selection and allocation to disrupted links in a network were made by Nurre et al. (2012), who develop a recovery process that determines which disrupted links to return to the problem, then optimally schedules their restoration based on the availability of work crews. Gong et al. [2013] study an interdependent supply chain network which integrates several underlying infrastructure networks (e.g., the power grid, communication, transportation), optimizing the cost of restoration and the performance of the multi-layer network. Shen [2013] develops a stochastic mixed integer model of the recovery of interdependent infrastructures under severe disruption. Baroud et al. [2014] develops a stochastic ordinal ranking approach to restoration of inland waterway networks based on two resilience-based importance measures from Barker et al. [2013].

3 PROBLEM DEFINITION AND STOCHASTIC OPTIMIZATION FORMULATION

The problem addresses a network □(□, □) consisting of a set of nodes □ and a set of links □. This network includes three categories of nodes: □□□ is the set of source nodes, □□□ is the set of sink nodes, and $N_□$ is the set of transmission nodes. The set □ contains different disruptive scenarios that can affect the network, each of which reduces the operability of links by some percentage. In the event of a disruption, the network is serviced by a supplier of □□ types of resources (e.g., some work crews have specific equipment, some crews have a certain number of works). The rate of recovery per unit of time is □. It is assumed that the rate of recovery for all links is equal, but the order in which a disrupted link is recovered affects the total restoration time of the network. The problem is described when a scenario disaster of type □ ∈ □, occurs, and it disrupts the links

proportionally from 0% to 100%. We must assign resources to disrupted links to lessen the percent of disruption. Then, the disrupted link are scheduled to be recovered one by one, and the order of recovery influences the total time of recovery.

Indices:

□, □ Indices of nodes in the network, □, □□$N = \{1, \dots, □\}$,

$$N = N_{□□} \cup N_{□i} \cup N_t, N_{so} = \{1, \dots, □_{so}\}, N_t = \{□_{so} + 1, \dots, n_t\}, N_t = \{n_t + 1, \dots, n_{si}\}$$

□ Index of resources available to be allocated to the disrupted links, $□ \epsilon K = \{1, \dots, n_□\}$

□ Set of scenario disasters which effect on network performance $□ \epsilon D = \{1, \dots, n_□\}$

o Index of the order in which a link is recovered, $o \epsilon \{1, \dots, n_o\}$

□ Index of stochastic scenarios, $□ \epsilon\ \Omega = \{1, \dots, n_\Omega\}$

Parameters:

n_o The number of disrupted links

$□_{ijd}$ The proportional damage to link (i, j) when disaster type d happens

$□_{ijkd}$ This is a factor whereby the vulnerability of link (i, j) is reduced when resource k is assigned to the link in the presence of disaster scenario type d

$□P_{ij}$ The nominal capacity of link (i, j)

$□o_{ijk}$ Cost of allocating resource k to (i, j)

$□□_k$ Cost of buying resource k

$□□_{ijd\theta}$ The cost of performance reduction in link (i, j) after disaster under scenario d occurs in scenario θ

$ℏ_{ijo\theta}$ The impact rate of link (i, j) recovery on network recovery when the link is recovered in the oth order

$□□_{ijo\theta}$ The cost of recovery link (i, j) in order oth in scenario θ

$□□_{id\theta}$ The penalty cost for supply production loss in the presence of disaster scenario d and under stochastic scenario θ

$□□_{id\theta}$ The penalty cost for demand loss in the presence of disaster scenario d and under stochastic scenario θ

$□_{k\theta}$ The aggregation number of resource of type k in scenario θ

□ The flow recovery per time unit in scenario θ

□ The time horizon for network recovery in scenario θ

□ The total available budget in scenario θ

$□_i$ The expected value of suppliers production at nodes $i \epsilon N_{so}$

D_i The demand expected to be satisfied at nodes $i \epsilon N_{si}$

$□_\theta$ The probability of stochastic scenario θ

Variables:

$□_{ijk\theta}$ $\begin{cases} 1 & \text{if resource } k \text{ is allocated to link } (i.j) \text{ in scenario } \theta \\ 0 & \text{otherwise} \end{cases}$

$□_{ijo\theta}$ $\begin{cases} 1 & \text{if link } (i, j) \text{ is recovered in the } o\text{th order in scenario } \theta \\ 0 & \text{otherwise} \end{cases}$

$□_{k\theta}$ $\begin{cases} 1 & \text{if we use resource } k \text{ for reducing vulnerability in scenario } \theta \\ 0 & \text{otherwise} \end{cases}$

$□_{ijdk\theta}$ The flow between (i, j) during disaster type d with resource k assigned for scenario θ

$□_{id\theta}$ The slack variable related to supply node i during disaster d under scenario θ

$□_{id\theta}$ The slack variable related to demand node i during disaster d under scenario θ

Based on the above notation, we formulate the multiobjective problem, which balances vulnerability and recoverability, as follows. The first objective function, provided in Eq. (1), minimizes aspects of vulnerability by minimizing (i) the percentage of performance decrease after the disruption, (ii) the cost of contracting with resource suppliers, (iii) the cost of assigning a resource to a link, (iv) the cost related to the time when a supplier produces the level of services or the amount commodities which is less than the expected level of services or

amount of commodities because of the disaster (the shortage in the amount of commodities or the level of the services a supplier provides), and (v) the cost of unmet demand in the network.

$$\begin{aligned}\min \sum_{\theta\in\Omega}\sum_{i\in N}\sum_{j\in N}\sum_{d\in D}\sum_{k\in\square} \square_{\theta} Cf_{ijd\theta}\square_{ijd}\square_{ijkd}\square_{ijk\theta}\square_{ijdk\theta} + \sum_{\theta\in\Omega}\sum_{k\in K}\square_{\theta} Cc_{k}\square_{k\theta} \\ - \sum_{\theta\in\Omega}\sum_{i\in N}\sum_{j\in N}\sum_{k\in K}\square_{\theta} Co_{ijk}\square_{ijk\theta} + \sum_{\theta\in\Omega}\sum_{d\in D}\sum_{i\in N}\pi_{\theta} LS_{id\theta}(S_i - \square_{id\theta}) \\ + \sum_{\theta\in\Omega}\sum_{d\in D}\sum_{i\in N}\pi_{\theta} LD_{id\theta}(D_i - \square_{id\theta}) \\ + \sum_{\theta\in\Omega}\sum_{j\in N}\sum_{i\in N}\sum_{k\in K}\sum_{d\in D}\sum_{o\in\square}\pi_{\theta} Cr_{ijo\theta}\left(\square_{ijd\theta}\square_{ijk\theta}\right)\square_{ijk\theta}\square_{ij\theta}\end{aligned} \tag{1}$$

The second objective function, provided in Eq. (2), maximizes the enhancement in recovery time for link (i,j) recovered in the oth order.

$$\max \sum_{\theta\in\Omega}\sum_{j\in N}\sum_{i\in N}\sum_{o\in\square}\sum_{d\in D}\sum_{k\in K}\frac{(\pi_{\theta} h_{ijo\theta}(1-\square_{ijl\theta}\square_{ijk\theta})Y_{ijk\theta}F_{ijdk\theta})}{\square}\square_{ijo\theta} \tag{2}$$

Constraint (3) ensures that a resource must be assigned to a link that is vulnerable to a disruption and potentially becomes disrupted when a disruptive event occurs. Constraint (4) matches repaired links with the appropriate number of resources, and Constraint (5) ensures that only disrupted nodes are repaired. Constraint (6) shows the resource usage limitation.

$$\sum_{k\in K} Y_{ijk\theta} \geq P_{ijd\theta} \qquad \forall i,j \in N, \forall d \in D, \forall \theta \in \Omega \tag{3}$$

$$\sum_{j\in N}\sum_{i\in N} Y_{ijk\theta} \geq \square_{k\theta} \qquad \forall k \in K, \forall \theta \in \Omega \tag{4}$$

$$\sum_{k\in K} \square_{k\theta} \geq P_{ijd\theta} \qquad \forall i,j \in N, \forall d \in D, \forall \theta \in \Omega \tag{5}$$

$$\sum_{j\in N}\sum_{i\in N} Y_{ijk\theta} \leq \square_{k\theta} \qquad \forall k \in K, \forall \theta \in \Omega \tag{6}$$

Constraints (7)-(9) calculate the amount of commodities and services that suppliers provide and target demands, as well as make sure that transmission nodes do not increase or decrease the amount of flow.

$$\sum_{j\in N}(1-P_{ijd\theta}I_{ijkd\theta})Y_{ijk\theta}F_{ijdk\theta} - \sum_{j\in N}(1-P_{ijd\theta}I_{ijkd\theta})Y_{ijk\theta}F_{jidk\theta} = \square_{idk\theta} \tag{7}$$
$$\forall i \in N_{so}, \forall k \in K, \forall d \in D, \forall \theta \in \Omega$$

$$\sum_{j\in N}(1-P_{ijd\theta}I_{ijkd\theta})Y_{ijk\theta}F_{ijdk\theta} - \sum_{j\in N}(1-P_{ijd\theta}I_{ijkd\theta})Y_{ijk\theta}F_{jidk\theta} = \square_{idk\theta} \tag{8}$$
$$\forall i \in N_{si}, \forall k \in K, \forall d \in D, \forall \theta \in \Omega$$

$$\sum_{j\in N}(1-P_{ijd\theta}I_{ijkd\theta})Y_{ijk\theta}F_{ijdk\theta} - \sum_{j\in N}(1-P_{ijd\theta}I_{ijkd\theta})Y_{ijk\theta}F_{jidk\theta} = 0 \tag{9}$$
$$\forall i \in N_{t}, \forall k \in K, \forall d \in D, \forall \theta \in \Omega$$

Constraints (10) and (11) represent supply and demand capacity limitations, respectively.

$$\square_{idk\theta} \leq S_{i\theta} \qquad \forall i \in N_{so}, \forall k \in K, \forall d \in D, \forall \theta \in \Omega \tag{10}$$

$$\square_{idk\theta} \leq D_{i\theta} \qquad \forall i \in N_{si}, \forall k \in K, \forall d \in D, \forall \theta \in \Omega \tag{11}$$

Constraint (12) requires that if link (i,j) is disrupted, at least one resource should be assign to it to reduce its vulnerability. Constraints (13) if an edge is disrupted by a disaster it should be recovered

$$\square_{ijo\theta} \leq \sum_{k \in K} Y_{ijk\theta} \qquad \forall (i,j) \in N, \forall k \in K, o \in \square, \forall \theta \in \Omega \tag{12}$$

$$\sum_{o \in O} \square_{ijo\theta} = 1 \qquad \forall (i,j) \in N, \forall k \in K, \forall \theta \in \Omega \tag{13}$$

Constraint (14) confirms flow capacity, constraint (15) represents the limitation on the recovery time horizon, and constraint (16) represents the limitation on the budget.

$$F_{ijkd\theta} \leq FP_{ij\theta} \qquad \forall (i,j) \in N, \forall k \in K, o \in O, \forall \theta \in \Omega \tag{14}$$

$$\max_{o=1}\left\{\sum_{i \in N}\sum_{j \in N}\sum_{k \in K}\sum_{d \in D}\left(\left(P_{ijdl\theta} I_{ijk\theta}\right) Y_{ijk\theta} F_{ijdlk\theta} \Big/ \square\right) X_{ijo\theta}\right\} + \cdots + \max_{o=\square}\left\{\sum_{i \in N}\sum_{j \in N}\sum_{k \in K}\sum_{d \in D}\left(\left(P_{ijdl\theta} I_{ijk\theta}\right) Y_{ijk\theta} F_{ijdlk\theta} \Big/ \lambda\right) X_{ijo\theta}\right\} \leq \square \qquad \forall \theta \in \Omega \tag{15}$$

$$\sum_{j \in N}\sum_{i \in N}\sum_{k \in K} Co_{ijk\theta} Y_{ijk\theta} + \sum_{j \in N}\sum_{i \in N}\sum_{o \in O} Cr_{ijo\theta} X_{ijo\theta} \leq \square \qquad \forall \theta \in \Omega \tag{16}$$

$$\begin{aligned} &Y_{ijk\theta}, X_{ijo\theta}, V_{k\theta} \epsilon \{0,1\} \\ &F_{ijdk\theta}, U_{id\theta}, W_{id\theta} \geq 0 \end{aligned} \qquad \forall (i,j) \in N, \forall k \in K, o \in O, \forall \theta \in \Omega \tag{17}$$

4 COMPUTATIONAL RESULTS

To develop stochastic optimization in the model, in vulnerability section, the cost of performance reduction in each link, the penalty costs, and the number of available resources are considered as uncertain parameters, and in the recovery section, the recovery cost and the rate of performance efficiency, when links are recovered in scheduled pattern, are considered as uncertain parameters. In order to model the problem under uncertainty the stochastic scenario based optimization is used in this paper. Let Ω be the set of all possible scenario and θ is a particular scenario. If π_θ denotes the probability of scenarioθ, because θ is a finite number (number of scenario is four,$\theta \in \{1,2,3,4\}$) the expected value function becomes a summation on θ. We consider four scenarios $\theta \in \{1,2,3,4\}$ which randomly are chosen to have a specific probability of occurrence. Each scenario has a determined set of parameters which lead to specified set of output for the model [Pishvaee et al. 2008].

Increasing the total number of scenarios can lead to a significant increase in the computation time [El-seyed et al. 2010]. Consequently, to limit the number of scenarios, a fuzzy clustering-based method presented by Pishvaee et al. [2008] was used to obtain a reasonable number of scenarios, in this case four scenarios, for a test problem shown in Table 1.

Table 0.1. The range of parameters for four different scenarios.

Scenario (θ)	Scenario probability (π_θ)	$Cf_{ijd\theta}$	$h_{ijo\theta}$	$Cr_{ijo\theta}$	$LS_{id\theta}$	$LD_{id\theta}$
1	0.4	~Unif[10,100]	~Unif[1,2]	~Unif[250,370]	~Unif[100,120]	~Unif[110,190]
2	0.3	~Unif[50,111]	~Unif[1.5,1.5]	~Unif[200,390]	~Unif[100,120]	~Unif[150,190]

3	0.2	~Unif[25,150]	~Unif[1,1.8]	~Unif[150,450]	~Unif[100,120]	~Unif[130,200]
4	0.1	~Unif[30,80]	~Unif[1.1,1.7]	~Unif[300,570]	~Unif[100,120]	~Unif[110,155]

For comparing the deterministic and the stochastic one is used as the nominal data for the deterministic model. Table 2 shows the experimental results of solving both deterministic and stochastic models and, moreover, depicts the reality that the stochastic objective function is more than that the deterministic objective function as the result of considering worst case situations, and the higher level of complexity as the result of having more constraints and decision variable having one more dimension.

Table 0.2. Computational result under nominal data.

Objective function	Optimal value of objective function		Number of variables		Number of constraints	
	Deterministic	Stochastic	Deterministic	Stochastic	Deterministic	Stochastic
	2889593	10543970				
Vulnerability(Obj.1)	2892070	10548584				
	2897416	10573195	240	957	357	1428
	8692506	29221055				
Recovery(Obj.2)	4346253	14610528				
	869250	2922106				

Figures 2 and 3 depict the Pareto optimal solution for both deterministic and stochastic models, respectively. As it is seen in Figure 3, the value of the vulnerability and recovery objectives have higher values than the objective functions for the deterministic model, suggesting that under different scenario with different probabilities, provides the model with the robustness whereby the model can tolerate abrupt changes in the parameters.

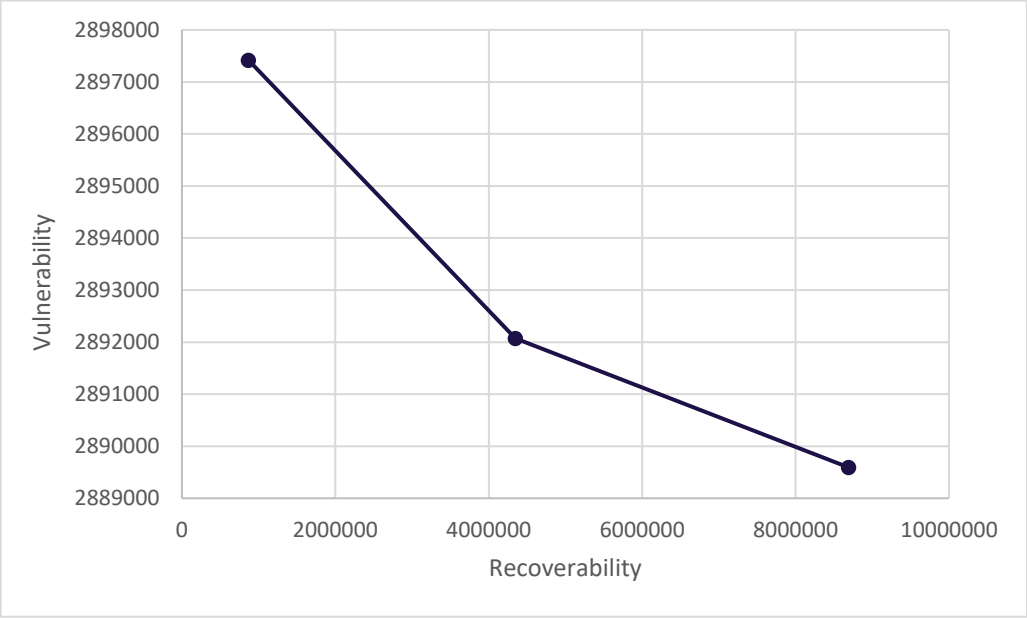


Figure 2. The Pareto optimal solution for deterministic model.

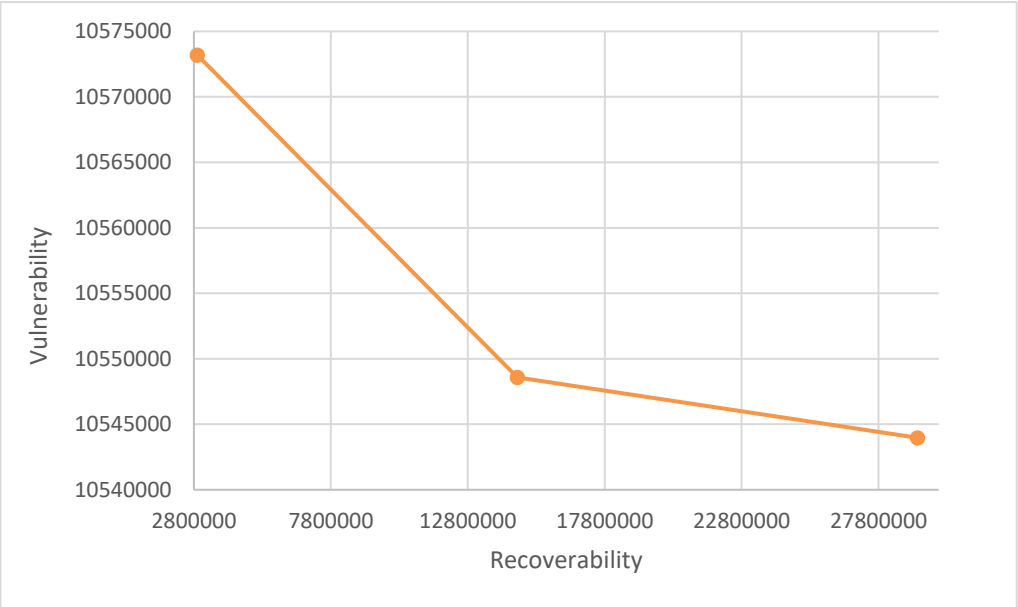


Figure 3. The Pareto-optimal solution for stochastic model.

5 CONCLUSIONS

This work provides a first step in developing an optimization framework for resource allocation to enhance network resilience wherein vulnerability and recoverability are treated as competing objectives. We offer a stochastic approach considering the parameter, which are inconstant in the real world, and make them flow easily in the distribution they follow instead of considering them as unique parameters. The results, both for deterministic and stochastic, depict the contradiction between two objective functions and furthermore, the higher results produced by the stochastic model and its ability to produce output under different scenarios shows the robustness of the stochastic model under the uncertain situation. Future work includes a more detailed analysis of multiple scenarios, as well as a data-driven study of real infrastructure network disruptions.

REFERENCES

Murray, A.T. and T.H. Grubesic. 2012. Critical infrastructure protection: The vulnerability conundrum. *Telematics and Informatics*, **29**(1): 56-65.

Barker, K., J.E. Ramirez-Marquez, and C.M. Rocco. 2013. Resilience-based network component importance measures. *Reliability Engineering and System Safety,* **117**: 89-97.

Barker, K., and H. Baroud. 2014. Proportional hazards models of infrastructure system recovery. *Reliability Engineering and System Safety*, **124**: 201-206.

Baroud, H., K. Barker, J.E. Ramirez-Marquez, and C.M. Rocco. 2014. Importance measures for inland waterway network resilience. *Transportation Research Part E*, **62**: 55-67.

Devanandham, H. and J.E. Ramirez-Marquez. 2012. Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering and System Safety*, **99**: 114-122.

El-Sayed, M., N. Afia, and A. El-Kharbotly. 2010. A stochastic model for forward reverse logistics network design under risk. *Computers and Industrial Engineering*, **58**: 423-31.

Gong, J., J.E. Mitchell, A. Krishnamurthy, and W.A. Wallace. 2014. An interdependent layered network model for a resilient supply chain. *Omega*, **46**: 104-116.

Hosseini, S., K. Barker, and J.E. Ramirez-Marquez. 2015. A Review of Definitions and Measures of System Resilience. In revision in *Reliability Engineering and System Safety*.

Lee, E., J.E. Mitchell, W.A. Wallace. 2007. Restoration of services in interdependent infrastructure systems: a network flows approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, **37**(6): 1303-1317.

Nurre, S.G., B. Cavdaroglu, J.E. Mitchell, T.C. Sharkey, and W.A. Wallace. 2012. Restoring infrastructure systems: An integrated network design and scheduling (INDS) problem. *European Journal of Operational Research*, **223**(3): 794-806.

Pant, R., K. Barker, J.E. Ramirez-Marquez, C.M. Rocco. 2014. Stochastic measures of resilience and their application to container terminals. *Computers and Industrial Engineering,* **70**: 183-194.

Pant, R., K. Barker, and C.W. Zobel. 2014. Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. *Reliability Engineering and System Safety*, **125**: 92-102.

Park, J., T.P. Seager, P.S.C. Rao, M. Convertino, and I. Linkov. 2013. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis*, **33**(3): 356-367.

Pishvaee, M.S., M. Fathi, and F. Jolai. 2008. A fuzzy clustering-based method for scenario analysis in strategic planning: the case of an Asian pharmaceutical company. *South African Journal of Business Management*, **39**: 15-25.

Shen, S. 2013. Optimizing designs and operations of a single network or multiple interdependent infrastructures under stochastic arc disruption. *Computers and Operations Research*, **40**(11): 2677-2688.

US National Academies of Science. 2012. *Disaster Resilience: A National Imperative*. Washington, DC: The National Academies Press.

Zolli, A. and A.M. Healy. 2012. *Resilience: Why Things Bounce Back*. New York, NY: Free Press.

ENGINEERING RESILIENCE TO POWER OUTAGES

Eric RIGAUD [1], Anouck ADROT[2], Frank FIEDRICH[3], Thomas MÜNZBERG[4],Wolfgang RASKOB[4], Frank SCHULTMANN[5], Marcus WIENS[5]

[1] MINES ParisTech, PSL Research University, CRC, Centre de recherche sur les risques et les crises, CS 10207 rue Claude Daunesse 06904 Sophia Antipolis Cedex, France

eric.rigaud@mines-paristech.fr / +334 93 95 74 86

Paris-Dauphine University, PSL Research University, Dauphine Recherches en Management DRM UMR CNRS 7088 Place du Maréchal Delattre de Tassigny, 75116 Paris Cedex

[2] anouck.adrot@dauphine.fr/ +33144054045

Wuppertal University, Institute for Public Safety and Emergency Management, Gaussstr. 20, 42119 Wuppertal, Germany

[3] fiedrich@uni-wuppertal.de / +49 202 31713280

Karlsruhe Institute of Technology (KIT), Institute for Nuclear and Energy Technologies Hermann-von-Helmholtz Platz 1, 76344 Eggenstein-Leopoldshafen, Germany

[4] thomas.muenzberg@kit.edu, wolfgang.raskob@kit.edu

Karlsruhe Institute of Technology (KIT), Institute for Industrial Production (IIP) Hertzstraße 16, 76187 Karlsruhe, Germany

[5] frank.schultmann@kit.edu, marcus.wiens@kit.edu

Abstract

The aim of the proposed paper is to apply resilience engineering thinking to power outages in the prospect of a definition of power blackout. This definition will support the development of a simulator based on a multi agent system and a guideline dedicated to the assessment and the enhancement of systems resilience to power outages.

Resilience engineering thinking refers to a new way to describe the dynamics of systems coping with threats and associated safety management system development. This approach aims to consider, among other, systems adaptive capacity to both anticipated and unanticipated situations and to support the development of associated safety management systems.

Power blackout refers to a short or long term loss of the electric power to a geographic area. Consequences of power outage depend, among other factors, on the duration of the loss of power and on the number of people and assets affected within the geographic area. As critical infrastructures are strongly interdependent, power outages can be a consequence and/ or a cause of other threats and consequently be part of a systemic crisis and disaster. However, the consequences of power blackouts have been persistently underestimated risks.

Applying resilience engineering thinking to power outages implies the definition of a four dimensional model. The first dimension refers to the system adaptive capacities to respond and recover to the occurrence of unwanted situations in general and to power outages in particular. The second dimension is related to the functions that support the improvement of adaptive capacities before and after occurrence of a threat. The third dimension refers to the diversity and the complexity of power outages threats. The fourth dimension concerns the short and long terms adaptive processes that stem from the reaction of the system to the occurrence of a power outage.

The design of this model will consider, among other factors, intrinsic properties of power outages (speed of onset, duration, area affected, etc.), systems connectivity and their potential escalation and propagation, adaptation processes to known situations and surprises, learning, monitoring and anticipating support functions, respond process and associated human and group dimensions.

The paper will be structured in three parts. The first part is dedicated to the presentation of power outage threats. The second part is related the presentation of the theoretical background of the model. The third and final part presents the model proposed.

REFERENCES

Boin A., Comfort L. K., Demchak C., 2010. The rise of resilience, in Comfort L.K., Boin A., Demchak C.C., (eds.), Designing resilience, preparing for extreme events, University of Pittsburgh Press.

Hollnagel E., 2011. Prologue: The Scope of Resilience Engineering, in Hollnagel E., Pariès J., Woods D. D. and Wreathall J., Resilience Engineering in Practice. Ashgate Studies in Resilience Engineering.

Münzberg T., Wiens M., Schultmann F., Dynamic-spatial Vulnerability Assessments: A Methodical Review for Decision Support in Emergency Planning for Power Outages, Humanitarian Technology: Science, Systems and Global Impact 2014, HumTech2014, Procedia Engineering, Volume 78, 2014, Pages 78–87

Woods D. D., 2006. Essential Characteristics of Resilience, in Hollnagel E., Woods D., Leveson N., Resilience Engineering: Concepts and Precepts, Ashgate.

PRACTICAL SAFETY, AN ETHICAL contribution TO RESILIENCE

Hortense Blazsin [1] and Franck Guarnieri [2]
[1] MINES ParisTech – PSL Research University, Rue Claude Daunesse, B.P 207, 06904 Sophia Antipolis Cedex, France
[1] hortense.blazsin@mines-paristech.fr
[2] MINES ParisTech – PSL Research University, Rue Claude Daunesse, B.P 207, 06904 Sophia Antipolis Cedex, France
[2] franck.guarnieri@mines-paristech.fr
http://www.crc.mines-paristech.fr/index-en.shtml

Abstract

As environments are becoming more and more complex, and less and less predictable, resilience and safety lie on ad hoc actions, decided by individuals in actual situations, in addition to adequate system design. We build on the work of a contemporary philosopher, Paul Ricoeur, to develop an approach of safety which articulates a system of rules with the confront them with the singularity of specific situations, through a process of "deliberation" which superior goal is to repect the principle of "solicitude" towards others, hence contributing to the ultimate goal of leading an ethical life. Such an approach requires that rules are applied autonomously by individuals, and that more broadly, they can express their "practical humanity". This possibility depends on the organizational environment in which they are set. Ricoeur calls the ideal-typical environment "just institution". We build on data gathered in the work practices of a gas distribution company to show that traces of practical humanity and deliberation are indeed present, although the organizational environment prevents them from developing fully. We term "practical safety" the approach of safety developed using Ricoeur's philsophy. A factor of "successful action", practical safety is favourable to organizational resilience.

1. INTRODUCTION

As Hollnagel has shown, (cf. for instance Hollnagel, 2014), in an unpredictable world, it is in specific situations that safety is preserved, thanks to successful action. Building resilient organizations therefore requires that the people who are the actors of these specific situations have the technical and behavioural skills to manage them adequately. Classically, "managing adequately" means preventing situations from cascading into a stage where they become out of control. It also designates the ability to regain control of a situation that has degraded up to that point, that needs to be brought back to a somewhat stable and functioning state, a process that is termed "entry into resilience" (Guarnieri, Travadel, 2014).

Yet, it seems a bargain to expect that people used to obeying general processes and rules established outside of them would all of a sudden be able to act and make decisions autonomously, as they have not had a chance to develop the necessary mechanisms prior to the situation where action is required (cf. Rasmussen, 1983). Therefore it is necessary for resilient organizations to articulate individuals' technical and behavioural ability to act adequately by themselves in specific situations, to their requirements in terms of stable rules and processes. Our point is similar to one expressed by Grote, on the necessity to find an optimal balance between stability and flexibility (Grote, 2014), that is built on learnings established by resilience engineering (cf. Hollnagel et al., 2006).

In a manner different from Grote's and resilience engineering's, we conceptualize the problem using a philosophical and ethical framework. To do so we call up to a French contemporary philosopher, Paul Ricoeur. We refer in particular to his concept of "practical reason", which can be quickly defined as reason anchored in an individual desire oriented towards an ethical goal. Underlying the concept is the articulation of morals and ethics, which confrontation culminates in practical wisdom. In a nutshell, according to Ricoeur morals and ethics are not essentially different. A distinction therefore has to be established through convention. According to the convention he sets, morals designate the rules that govern individuals' daily actions. Ethics correspond to the superior aim to achieve "a good life, with and for others, within just institutions" (Ricoeur, 1992). Aiming a good, ethical life is what allows individuals to fulfil their human nature. Moral rules are applied autonomously, i.e. recognized by individuals as justified and adequate to indeed act in a manner that achieves an ethical life, which they can therefore interiorize as rules they have given to themselves. In daily situations and relatively situations, they suffice to achieve this aim. There are also moments when the "tragic of action" surfaces, i.e. when rules contradict themselves, or when no rule exists to guide action in a specific situation. In such situations individuals have to carry out a process of "deliberation", i.e. confront rules that may apply (but do not) to the overarching ethical principle of "solicitude" towards others. At the end of this process of confrontation, a decision is reached

that can be considered a result of "practical wisdom". Practical reason, the morals / ethics articulation, deliberation and practical wisdom are part of a broader conceptual framework that may be termed "practical humanity". Practical humanity refers to a set of sentiments, such as self-respect and solicitude, and acts, such as practical reasoning, hermeneutic analysis or deliberation (N.B: the list is non-exhaustive), that help achieve an ethical life, and conversely are signs that the individual is indeed following this path. Finally according to Ricoeur, depending on the "institutional" (i.e. organizational) environment, practical humanity is more or less favoured and subsequently, likely to be expressed. He calls the ideal-typical environment "just institution".

In our article we defend the idea that Paul Ricoeur's practical humanity offers a heuristic to conceptualize safety preservation and helps shed a new light on such issues as the articulation of individual, autonomous action, with set organizational processes and rules. We believe it could help strengthen resilience engineering, by engaging a dialogue on how individuals can carry out "successful actions" and therefore, contribute to the preservation of safety, organizational stability and ultimately, resilience. Furthermore the model of "just institution" could help shed a different light on the stakes underlying the conception of resilient organizations. Building on data gathered in a gas distribution company, we show that Ricoeur's philosophy is not only heuristic, but also anchored in tangible safety practices. First, we outline the methodology used to gather data, the organizational environment in which they were collected. Then we describe and analyze cases where workers have carried out a process that contains germs of deliberation. Finally, we show the many ways in which Ricoeur's practical humanity can provide a heuristic for safety preservation, and even give birth to a new approach of safety that we term "practical safety" (Blazsin, 2014).

2. INDIVIDUAL INTERVIEWS TO IDENTIFY TRACES OF PRACTICAL REASON IN THE PRACTICES OF WORKERS AT THE SHARP-END OF A GAS DISTRIBUTION COMPANY

The idea that Ricoeur's practical philosophy could offer not only a heuristic, but also tangible tools to develop a new approach of safety preservation, had to be confronted with field realities. This was carried thanks to an industrial partner, a French gas distribution company. We focused on the company's core activity, i.e. operating the gas distribution network. Following an initial 5-week phase of non-participant on-site observation, twenty-one interviews were carried out in order to dig deeper into the way workers experience their work and safety practices and possibly, identify traces of practical humanity.

2.1 Gas distribution, an old trade relying more and more on procedures and organizational work

Our research was carried out in partnership with a large gas distribution company, which is responsible for the delivery of natural gas from the transport network to the end-user. To do this, it must operate and maintain nearly 200,000 km of pipeline. This involves: monitoring the status of the network and carrying out any maintenance operations that are necessary to avoid leaks; connecting new customers (expanding the network, creating connections); disconnecting parts of the network (removing connections, regulators, sections of pipeline); finally, coordinating with other companies whose activities may have an impact on gas installations.

We decided to focus research on operations, which is both the company's central and oldest activity. As such it has been subjected to many transformations, from a technical, procedure and subsequently cultural perspective. Therefore it seemed relevant to try and access the profound level of identity and behaviour that Ricoeur describes. Indeed considering that practical humanity is an essential (in the strongest sense of the word) component of the individual, it should not be impacted by variations on techniques or representations. Therefore a changing environment may be considered as a test by itself.

What's more the operations department is also where workers are confronted with everyday safety preoccupations. Indeed they work in an open environment surrounded by people who may suffer from the consequences of an accident. Similarly, if their intervention on the network is not carried out correctly, it may trigger to harmful consequences in the mid or long term, for instance by leaving a small leak on the network which will progressively accumulate in a nearby building and possibly, in extreme circumstances, lead to an explosion. Yet in comparison with the safety stakes, the actual work that has to be carried out requires very little technical expertise. Workers carry out such operations as creating or deleting connections. An important part of their job is also to carry out maintenance operations, such as checking that a network valve is indeed accessible for manoeuvre in case it is needed, for instance to stop the gas flow from coming in a specific part of the network if there is a leak. Such an act is obviously simultaneously crucial for safety, all the while requiring hardly any technical skill. Therefore although this is particularly true for valve checking, overall, operations now rely more and more on procedures and less and less on technical expertise. The situation raises a challenge in terms of meaning, and implication.

In addition to the importance of operations for the industrial partner, the gap between safety and actual work made it particularly interesting to study, as one could assume that all that remained for workers to be stay alert on safety issues was their consciousness of the potential consequences of their actions on third parties – ultimately, their humanity. Therefore it made sense to try and understand how this humanity is practically expressed, through sentiments, ideas and actions, to preserve safety.

2.2 Individual interviews, an opportunity to move beyond collective representations, into personal experience of the field

To carry out our research project, a phase of non-participant on-site observation was first carried out. Three sites were observed, in order to balance the limitations resulting from an anchor in a specific territory, with its technical as well as cultural history, its specific team dynamic, etc. This phase was crucial to develop an understanding of gas distribution as a technical and organizational activity, the way it is carried out, impediments the teams face and the way those are dealt with. Yet it was insufficient to dig deeper into the way workers experienced their work, their relationship with safety, and possibly expressed their practical humanity.

To do so, twenty-one interviews were carried out with field-level workers. The group included twelve "operators", i.e. those workers who carry out the actual fieldwork; five "chief of operations", who are in charge of ensuring that operations do not impact the rest of the network and are in line with procedures; four "team managers" and "preparers", who respectively manage the team of operators from an HR perspective (affectations, holidays, trainings, etc.) and prepare the fieldwork (technique, procedures, administrative work, etc.). This distribution reflects the way teams are structured in real life.

Interviews were semi-structured, carried out individually, and revolved around workers' representations of their work, the organisation, their individual and collective contribution to safety. An important part of the interviews was dedicated to asking them to reflect on past experiences that had left on mark on them, where they thought they had "acted well" or on the contrary, where they thought they had made a mistake.

2.3 An ad hoc grid analysis to identify traces of practical humanity

To analyse the data hence collected and identify potential traces of practical humanity, an ad hoc grid analysis was developed, using the main components described by Ricoeur as composing it. The below figure (figure 1) is a screenshot showing the way the data was treated:

	Ethical sentiments			Ethical acts				Standards of excellence
	Desires, motivations, motives	Self-respect, Self-esteem	Respect of others, solicitude	Hermeneutic analysis	Practical Team manager asoning	Narrative configuration	Deliberation	
Operator 1								xx
Operator 2	x	x	x			x		xxxx
Operator 3	xxxxxx	x	xx		x	xx		xx
Operator 4	xxxx					x		xx
Operator 5	x							xx
Operator 6	x				x	x		x
Operator 7	x	xxx				xx		xx
Operator 8	xxx	xx	x		xx	xx		xxxx
Operator 9	x					xx		xxxx
Operator 10			xxx			xx	xx	xx

Figure 1. Analysis grid developed using Ricoeur's "practical humanity".

The three main categories composing practical humanity are "Ethical sentiments", "Ethical acts" and "Standards of Excellence". The latter, that are not so to speak qualities, ensue from the work of another contemporary philosopher, Alastair MacIntyre. Ricoeur calls up to him to build his practical philosophy. MacIntyre defines practice as "any coherent and complex form of socially established cooperative human activity through which goods internal to that form of activity are realized in the course of trying to achieve those *standards of excellence*[5] which are appropriate to, and partially definitive of, that form of activity" (MacIntyre, 2007, p.187).

[5] Our highlight.

Standards of excellence therefore offer a heuristic to analyse a profession and, in our case, determine whether safety preservation appears as a central feature.
In order to address the question raised during this symposium, regarding the matter of adaptability and (un)predictability, we will focus the rest of the article on one specific item of this grid, namely the instances of "deliberation" which were traced in the discourse of interviewees. Indeed as mentioned, deliberation is the activity where rules and context are explicitly articulated and confronted, if rules do not apply. It is therefore the most relevant to determine whether interviewees demonstrate conscious adaptability in their work and safety practices and if so, what form it takes. We consider being "conscious" of adapting as a key aspect of relevant adaptation, as it appears to be the only way for workers to remain aware of straying from the initial plan and therefore, ensuring that they evaluate the potential consequences of such straying.

3. DELIBERATION, A RARE BUT EXISTING PRACTICE WHEN RULES CAN'T BE FITTED TO SITUATIONS

Deliberation is the process through which general, moral rules are confronted with specific situations. Ultimately, it leads to "practical wisdom", which Ricoeur defines as resulting from "situated moral judgment", (Ricoeur, 1991, p.281), which consists of "inventing the just behaviours adapted to the singularity of cases"[6] (ibid., p.313). Far from being arbitrary, the confrontation of general rules to specific situations results in practical wisdom thanks to the overarching aim of the "good life" and specifically, solicitude towards others. Translated into safety-friendly terms, this relates to the adaptibility of general rules to unexpected situations and ultimately, to the flexibility / stability balanced mentioned in this paper's introduction.

3.1 Deliberation, primarily a managers' thing

Six instances of deliberation were identified in the data, mentioned by four interviewees. This is a small sample. As a comparison, fifteen interviewees mentioned twenty-four instances of hermeneutic analysis, which is the ethical act best represented in the data that was collected. Generally, ethical sentiments gathered more instances than ethical acts[7].

However few, some instances of deliberation were still identified in the data. One operator, two chief of operations and one team manager expressed them. There is one additional mention (which is not part of the count) where a second operator mentions the necessity to confront rules to situations where they cannot be applied and to determine an ad hoc solution, which he says is the responsibility of the chief of operations, therefore disengaging himself from the process and associated responsibility.

The two instances mentioned by the operator focus on the perceived conflict opposing two general principles, one that could be termed "duty" or "job well done", and the other being immediate safety. The two chief of operations develop a general discourse on the fact that by definition, rules can't be applied to all specific situations; when they don't apply, the safety of workers takes precedence without question. Finally, the team manager comments on the fact that general rules are subject to different interpretations and that it is necessary to confront them with field situations and tangible goals, such as being able to stop the gas from flowing in case a fire occurs, to interpret these rules in an appropriate manner.

3.2 Deliberation, a relative rarity to be accounted for

Two main elements emerge from this description of deliberation instances. First, the fact that it is to be found primarily in the discourse of managers leads to thinking that deliberation requires some level of perceived liberty to question and possibly, bend the rules conceived by the organization. Second, the fact that there are so few instances is astonishing, compared with the abundant documentation provided by the Safety Sciences

[6] Our translation.

[7] Ethical sentiments were identified as follows: 28 instances of respect for others / solicitude mentioned by 14 interviewees; 26 desires / motives by 13 interviewees; 12 expressions of self-respect / self-esteem mentioned by 9 interviewees; amounting to a total of 66 instances.
Ethical acts were identified as follows: 24 instances of hermeneutic analysis by 15 interviewees; 10 instances of practical reasoning by 6 interviewees; 6 instances of narrative configuration by 5 interviews; 6 instances of deliberation by 4 interviewees; amounting to a total of 46 instances.
Finally, let's note that the sole "Standards of excellence" category gathers 50 instances, mentioned by 15 interviewees. This both attests to an existing "ideal" of the profession, and needs to be related with the low number of expressions of self-esteem and narrative configuration, which may be interpreted as a difficulty to relate the ideal model of work with actual, experienced practices.

community (cf. for instance Marais, Dulac & Leveson, 2004 ; Hollnagel, Woods, Leveson, 2006 ; Hayes, 2013). This second point is to be related to the many instances which were not counted as "deliberation", where interviewees denied the necessity to confront rules with situations as in any case safety is what primes, a self-sufficient rule rendering any attempt at confrontation useless.

We interpret them as confirming the relevance of practical humanity to conceptualize safety preservation and of its dependence on the institutional / organizational environment. Indeed, it fits Ricoeur's conceptual model, according to which the just institution is key to express practical humanity, deliberation included. As current organizations are based on rational, engineered models (cf. Blazsin, 2014), at odds with the ideal-typical jus institution, one may conclude that it is indeed the organizational environment that is responsible for sentiments not being translated into actions.

Furthermore, the fact that safety is considered as an overarching principle, without its tangible, situated implications being even questioned, may be considered as counterproductive in terms of safety. Indeed it leads to apply this principle without having confronted it with its relevance, to it being obeyed as ensuing from an outside order and therefore, to safety resting on an heteronomous, rather than autonomous, dynamic.

4. CONCLUSION

In this paper we have endeavoured to illustrate the relevance of Ricoeur's conceptual framework of "practical humanity" by focusing on one of its specific components, "deliberation". In our perspective deliberation offers a heuristic to analyse the question of situated tradeoffs, which resonates with the necessity to reach a balance between flexibility and stability at the organizational level. By conceptualizing an articulation of general rules with a superior, ethical aim, which provides guidance when general rules are confronted with singular cases and do not apply, Ricoeur offers a way out, and even a way up, to preserve safety and strengthen resilience.

Indeed in his perspective, general rules are conceived to help individuals reach "the good life for oneself and with others within just institutions", i.e. excellence in their practice leading to self-respect and solicitude towards others, allowing for self-esteem. As such, the worth of rules is not intrinsic. On the contrary it lies on their ability to guide situated, singular action towards the good life. Furthermore, aiming the good life is a fundamentally individual path, necessary for a person to fulfil its human nature and as such, anchored in what one deeply wants to build for one's life. Therefore the rules to be followed cannot come from an outside source and be obeyed out of sheer respect for authority. They need to be truly experienced as just, and therefore adequate to achieve this essential aim. Consequently they can only be *autonomous* rules, ones that the individual has confronted to ethics and recognized as indeed adequate to achieve the good life. One telling example of how essential autonomy is to resilience can be found when reflecting on the Fukushima Daiichi disaster. At the time, a team of workers decided to remain at the plant in order to contain damage (cf. Guarnieri et al., 2015). Making the decision to sacrifice one's own life in order to save others is likely the strongest form solicitude can take, and it cannot be enforced by an outer source of authority. This is particularly true in such extreme situations, where all pre-existing systems of rules, including symbolic ones, collapse. This illustrates the role played by individuals' inner will, i.e. autonomy, in the management of such situations, and the essential role it plays to enter into resilience and regain some level of stability. Therefore through his articulation of morals and ethics, Ricoeur provides us with an opportunity to conceive systems of rules that can be applied in a truly autonomous manner, favouring implication to obey them, and that individuals have the liberty to question and possibly, bend them, should the situation requires so. As such, he offers a key to help build more resilient organizations.

Obviously, such an approach of rules and autonomy requires a radical shift in the way organizations currently manage these rules, and the people applying them on the field. This is consistent with Ricoeur's theory of the just institution. More broadly, it provides a tangible proof point in favour of Ricoeur's practical humanity and its relevance to shed a new light on safety preservation and organizational resilience. Such items as solicitude towards others and standards of excellence offered intuitive motives to postulate its relevance. What has been said on the importance of autonomy to build a system of rules that would be simultaneously stable, and allowing for ad hoc action, combined with the profoundly intimate relationship between moral rules and the ethical aim of leading a good life, offers the possibility to renew the way we conceive individual implication in the preservation of safety within organizations. We term this new way "practical safety", and propose a tentative definition according to which practical safety is "the ability of individuals to appropriate safety as an internal value, which enables them to decide on a course of action that preserves the safety of others as well as their own, when a situation requires them to do so". Such an approach asserts the idea that safety can only be managed by people in organizations, rather than by organizations through people. It offers a way to tie together the autonomy indispensable to situated action with a coherent system of rules, hence addressing the question of adaptability in unpredictable environments: in this perspective, predictability is no longer an issue. It also

provides an opportunity to renew individual engagement for safety and therefore favour attention and implication, which are key to organizational resilience.

Acknowledgements

We would particularly like to thank TOTAL, GDF SUEZ, SNCF and AFNOR, who are the partners of the Mines ParisTech Resilience Engineering Chair. These companies sponsored this research and thereby contributed to the creation of knowledge in the field of industrial risks.

REFERENCES

Blazsin, H. (2014). “De l’ingénierie de la raison à la raison pratique : vers une nouvelle approche de la sécurité”, Doctoral Thesis, Ecole des Mines de Paris.

Grote, G. (2015). “Promoting safety by increasing uncertainty – Implications for risk management”, Safety Science 71, pp.71-79.

Guarnieri, F. and Travadel, S. (2014), ‘Engineering thinking in emergency situations: A new nuclear safety concept’, Bulletin of the Atomic Scientists, Volume 70, Number 6, pp. 79–86

Guarnieri, F., Travadel, S., Martin, C., Portelli, A.,, Afrouss, A. (2015). L’accident de Fukushima Dai Ichi, Le récit du directeur de la centrale. Vol. 1 L’anéantissement, Presses des MINES.

Hayes, J. (2013). Operation Decision-Making in High-Hazard Organizations: Drawing a Line in the Sand, Ashgate.

Hollnagel, E., Woods, D., Leveson, N. (2006), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, UK.

Hollnagel, E. (2014). Safety-I and Safety-II. The Past and Future of Safety Management, Ashgate.

MacIntyre, A., (2007 (1981)). After Virtue. A Study in Moral Theory, Notre Dame: University of Notre Dame Press, Indiana.

Marais, K, Dulac, N, Leveson, N. (2004), “Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems”, Engineering Systems Division Symposium.

Rasmussen, J. (1983). “Skills, Rules and Knowledge; Signals, Signs and Symbols, and Other Distinctions in Human Performance Models”, IEEE Transactions on Systems, Man, and Cybernetics 3.

Ricoeur, P. (1991 (1986)). From Text to Action: Essays in Hermeneutics II, trans. Blamey, K., Thompson J. B., Evanston: Northwestern University Press.

Ricoeur, P. (1992 (1990)). Oneself as Another, trans. Kathleen Blamey, Chicago: University of Chicago Press.

Weick, K. E. (1995). Sensemaking in organizations, Foundations for Organizational Sciences, Sage.

DISASTERS, COMMUNITY SPONTANEOUS ACTIONS, AND COMMUNITY RESILIENCE

Jane Ciambele Souza da Silva[1], Ricardo José Matos de Carvalho[1]
and Paulo Victor Rodrigues de Carvalho[2]
[1]Universidade Federal do Rio Grande do Norte, Natal, Brazil
[1]jane_ciambele@hotmail.com, rijmatos@gmail.com
[2]Instituto de Engenharia Nuclear, Rio de Janeiro, Brazil
[2]paulov195617@gmail.com

Abstract

This work aims to analyze how the spontaneous actions implemented by members of the community in a post-disaster situation help to promote community resilience and prepares the community to deal with new disasters. The field study was done after the disaster in the Mãe Luiza community, due to heavy rains that hit the city of Natal, in June 2014. The disaster was a landslide that culminated in a huge crater that affected more than 180 families. The field research uses ethnographic methods based on ergonomics Community Ergonomics framework. The researches facilitate the meetings held by community members after the disaster. These meetings were an important space for the disaster victims obtain guidance; identify and organize their real demands; discuss and decide on the strategies to be adopted; bring government officials and technicians for the community to clarify, discuss and solve problems; involve community leaders; to schedule a public hearing in the municipal parliament; experience the collective participation, reflect and learn from their own experiences, and; monitor the decisions and measures taken by the authorities. We conclude that the meeting space enhance the community resilience, empowering the community to take collective actions to solve problems based on their knowledge of the situation, instead of waiting for top down solutions coming from authorities.

1 INTRODUCTION

The community of Mãe Luiza, located in the east of the city of Natal, northeast of Brazil, suffer with a landslide caused by heavy rains that hit the city in June 2014. The slide occurred in a region formed by high altitude dunes and culminated in the formation of a crater that has 10,000 m^2 and 30 m deep, as shown in Figure 1. According to the information provided by the Municipal Labor and Social Welfare authority – SEMTAS, the disaster affected more than 180 families, of which 28 had their homes completely destroyed.

Aware of the impact those disasters can cause the United Nations Office for Disaster Risk Reduction - UNISDR has developed and implemented actions to reduce the risks of disasters and promote community resilience in the cities, based in an ethic of prevention (UNISDR, 2015). The actions planned by the UNISDR (2012) are based on the Hyogo Framework for Action - MAH (2005-2015), which defines the conditions for a safer world by 2015.

Based on this Marco, Brazil enacted in 2012 the Law No. 12,608, made the federal government, the states and municipalities responsible for the implementation of actions to reduce the risks of disasters and promote community resilience. The law also encourages community participation in risk management to ensure the effectiveness of actions. Nevertheless, many cities in Brazil do not yet have their own strategies, plans and programs for disaster risk reduction, such as the city of Natal. Natal does not have a contingency plan, although it has many areas considered at high disaster risk like Mãe Luiza neighborhood itself.

The objective of this field study in Mãe Luiza, based on Community Ergonomics framework, is to show how the collective knowledge and spontaneous actions developed by members of this community in a post-disaster situation contribute to promote community resilience and prepares community to deal with events of major proportions.

Figure 1. Crater in Mãe Luíza.source: Project Viva Mãe Luíza.Available in: https://projetovivamaeluiza.wordpress.com/2014/06/

2 THEORECTICAL BACKGROUND

2.1 Disasters

As described in the report by the International Strategy for Disaster Risk Reduction - ISDR (2002), disasters can be understood as a serious disruption of the functioning of a community / society causing loss of life, material, economic and environmental, exceeding community capacity / affected society to cope with the situation using their own resources. "The disaster is a function of the risk process" and "results from the combination of hazards, conditions of vulnerability and insufficient capacity or measures to reduce the potential consequences of risk" (ISDR, 2002, p. 38).

Quarantelli (1988b) proposes that the current paradigm of research on disasters is guided by two main ideas: 1) disasters are an inherently social phenomena and natural events such as hurricanes or storms are not the disaster itself, but the source of the damage; 2) the disaster is rooted in the social structure and reflects social change processes. It is understood from this view that the disaster "is not a physical event (...), is a social occasion."

Therefore, it seems inappropriate to allocate to disasters the term "natural" as if they could happen out of human actions and decisions and their communities (Quarantelli, 1988). Therefore, one can understand that the location in risk areas and even the way of life of the poorest communities, such as Mãe Luiza, serve to exacerbate the negative effects of disasters. Quarantelli (1988) also explains that humans are, in a way, "those responsible for vulnerability" and that "if there are no negative social consequences, there is no disaster." However, according to resilience engineering principles, success and failure is the flip side of same coin (Hollnagel, 2010) and, if the society was not able to provide better living solutions for poor people, there is a need to discover and enhance ways in which people actions can improve resilience in their communities.

2.2 Community Resilience

Hollnagel and Woods (2006) define Resilience Engineering (RE) as "a paradigm for safety management that focuses on how to help people cope with the complexity under pressure to succeed." The RE approach has been focused on safety critical industry applications. However, more recently, the Resilient Cities framework appeared as a strategy to manage risk in cities ISDR (2002), considering that hazards that can cause accidents and disasters, understood often unpredictable, dynamic, and complex events. Even considering the these two views of resilience came from different basic concepts, it is important to note that both aim to improve the adaptive capacity of systems when face major disruptions.

A system should only be called resilient "when it is tuned such that it can use their potential abilities, engineering resources acquired or adaptive skills, the maximum length and in a controlled way, both expected and unexpected situations. A measure of resilience is therefore the ability to create forecast - to anticipate the shape change or risk of failures and before damage occurs" (Hollnagel and Woods, 2006).

Hollnagel (2010) defines resilience as the intrinsic ability of a system to set their operation before, during or after changes and disturbances.

According to Kulig et al. (2008) Community Resilience can be understood as a theoretical framework and social process able to explain how communities develop resilient responses to external forces, as well as economic crises, disasters and other threats to sustainability. Therefore, developing community resilience requires that communities become involved and develop a set of best practices that enable them to resist, adapt and recover from a disaster situation. Thus, it is believed that the responsibility for disaster risk reduction is a mission that involves everyone, and ethics and humanism principles and solidarity, should be part of daily life, from the way the young are educated to way we plan our cities (Carvalho et al, 2013).

2.3 Community participation

According to Rodrigues (2010) the actions proposed by the UNISDR are essential tools for reducing disaster risks and promoting global community resilience. However, this concern does not translate in practice in most countries, whose actions that contribute to the UNISDR objectives are neglected.

In Brazil, it is known that the official system for disaster risk management in cities has shown flaws in all phases, and that the populations of vulnerable communities are not involved and properly prepared on how to act resiliently in a disaster situation. Also, the top-down approach for developing contingency plans are based on forced action of civil defense and policy agents, where people from the communities are viewed as passive element to be removed, instead of active actors in the process. This situation enhances the distrust that already exists among people and agents – due the violent background of many communities – minimizing the possibilities of success of disaster response actions.

The top-down approach and non-involvement of the community people is rooted in ideas coming from traditional safety paradigm in which there are “best ways” to develop a response plan, that there are specialists to develop the plans, and that the ordinary people are morons and cannot contribute to the plan. Therefore the approach does not encourage early and cooperative participation of communities during the phases of the management of disaster risks. Chan (2013) believes that this top-down approach to disaster risk management has been the reason for failures in many response actions systems, and she claim that a bottom-up action approach, which focus on the opportunity to engage individuals in management actions, can help to increase the resilience of communities.

In the same way ISDR (2002) considers that the measures to reduce disaster risk function better when they involve the direct participation of the community. Although there are indications that the community participation is important, in practice, at least in Brazil, community people is almost completely away from the decision-making process involving their welfare and protection.

There are enough experiences that prove that the participation of residents in actions involving the reduction of disaster risk in their communities can be very effective if given the proper care and have the necessary resources (ISDR, 2002). It is necessary to educate communities about the importance that risk reduction processes and actions have for their well-being. Moreover, it is necessary to define and transmit the knowledge reflecting the practice of risk management, strengthening local capacity to identify threats and local response possibilities, and improving the livelihood of residents (ISDR, 2002).

It can be seen that the actuation of the people from communities is at the heart of an adequate risk management system in all its phases (pre-disaster, disaster and post-disaster). People local knowledge is a crucial factor in ensuring the efficiency of response actions, increasing the community resilience.

3 METHOD

The research was done under the Ergonomic City or Ergopolis project (Carvalho, 2012) based in the Community Ergonomics framework. Tis framework is based on the principles of participation and involvement of community members in the decision-making processes and actions regarding to their community. The Community Ergonomics takes a participatory and grounded approach aiming the creation of spaces and forms of collective dialogue, providing spaces for community members discuss and solve their problems (Schmitz, 2000).

Understanding participation as an important aspect of Ergonomics is already known. According to Darses et al. (2007) participation "contributes to personal development" (...) "and will only be effective and efficient if the persons involved have individual interest to participate and have their participatory efforts rewarded." For them, only participation is not enough to achieve success, while it needs to take in account social and individual requirements and needs to be a way to develop collective action. In addition, participation also contributes to the "skills development" (Darses et al. 2007) and for improving communication and integration between individuals.

During this research, ergonomists act as facilitators and sometimes moderators of the internal meetings of the members of Mãe Luiza community and meetings of community members with public authorities. These meetings had audiovisual record with the permission of all participants. The aims of these meetings were listen reports and organize demands of the community members, regarding the disaster consequences, discuss them and decide on the strategies and actions. Figures 2 shows one internal meeting in Mãe Luiza and Figure 3 shows a meeting in the town council.

The research subjects are all community members affected by the disaster, i.e. people who had their houses totally destroyed, damaged or interdicted by the Department of Social Protection and Natal Civil Defense and attended the meetings. Some of these individuals witnessed the disaster site and contributed in describing the details involving the pre-disaster phases, disaster response, and post-disaster.

Figure 2.Mãe Luíza internal meeting.

Figure 3. Meeting in the town council.

During the research we also use secondary information sources about the disaster coming from videos from local and national TV stations and social media. Using the records of these meetings, interviews with community members and authorities, and the secondary information sources we were able to identify the problems that occurred during the disaster response and recovery and also the actions taken by community members to address their problems.

4 RESULTS

Problems reported by the community meetings revealed unpreparedness of Civil Defense and the Fire Department during the pre-disaster and response phases. The absence of appropriate an efficient equipment to support basic actions, such as remove garbage from sewer pipes, led people from community to act on its own and without the necessary qualification, as shown in Figure 4,where locals trying to set the water protection canvas at the disaster site, putting their own life at risk. During recovery phase, the problems reported by residents in the meetings were related to water supply, power supply, housing assistance, recovery and reconstruction of housing, transportation, security, health and social care. Besides the problems were identified the strategies undertaken by people in the community for decision-making and problem solving based on the speech of individuals at all stages of disaster management. The detailed description of these strategies and actions falls out of the scope of this paper.

It is noticed that the collective / participatory activities performed by disaster victims and between them and the public and the scientific community, creating a new space to promote resilience in the community because people who participate in these actions may: get information on the real situation in which they are and clarify conflicting information; get directions; identify and organize their real demands, discuss and decide on the best strategies to be taken; bring the authorities and technicians for the community to clarify, discuss and solve problems; engage community leaders; schedule a public hearing in the town council; being heard by the authorities and the media; understand what a disaster is and what actions need to be taken in the view of this type of event (heavy rain and landslide); establish alliances with sectors of society; experience solidarity, cooperation, consensus, dissent, frustration, hope; reflect and learn from their experiences; stay organized; monitor the decisions and actions of the authorities; seek to know how the civil defense work in other cities and examples of success; start creating knowledge about the national disaster policy and legislation, and national

and international guidelines; exercise, along with civil defense agents, perceive the importance in participate in disaster simulations exercises, and; develop collective knowledge.

Figure 4.Locals trying to set the water protection canvas at the disaster site.

Therefore, the meetings and the emergent collective space for decisions and actions performed by residents as allowed the exchange of experience, progressive learning, and contributed to the development of a way to deal with disaster risks being more resilient. The people involved were also able to understand and reflect on the first or weak signals of disaster, enabling more actions possibilities in order to avoid or to be alert about dangerous situations, before the occurrence of the disaster. They could also create collective alliances with other sectors of society, who are capable to help in handling disasters and contribute to the improvement of life in their community. It was also perceived that these actions have provided increased citizenship and result in a gradual improvement in the community resilience to disasters.

5 CONCLUSIONS

The lack of a contingency plan in the city that encourages community participation in disaster risk management may lead to disharmonies in response actions to disasters. In addition, this research pointed out the lack of preparation and organization planning of Civil Defense and other agencies related to civil protection, the inefficiency of town hall and other bodies responsible for disaster management, which led community members to act often on their own and without the qualification required. On the other hand, even without possessing proper qualification, some actions taken by the community before, during and after the disaster showed the initiative of residents to solve problems, and the importance of community collective action. These actions also indicate that there is a certain community resilience potential that can contribute to increased global community resilience if proper treated by the authorities.

The Community Ergonomics frame work stressed the importance of involvement and participation of the actors in actions aimed at promoting the resilience of the community. Within this context of participation it is important to note that the role of the ergonomists as facilitators and moderators at the meetings, in guiding victims about the decisions to be taken, and the in the strategies that need to be taken.

Finally, we concluded that the positive spontaneous actions promoted by the community can be recognized and legitimized by the authorities in the preparation of policies, guidelines and planning actions against risks and disasters. We also conclude that the meetings held by the community has become a collective conversation space in which all participants were able to talk and reflect on their reality, decide on their demands and strategies to ensure their rights, allowing participants to be more aware about this condition in relation to the possibility of new disasters. They perceived that when acting collectively they are better able to manage the impacts caused by the phenomenon. The creation of a space that provide knowledge and experience sharing and the collective exercise of citizenship, enable some achievements to the community, and an environment that may afford the gradual improvement of the community resilience.

Acknowledgements

The authors would like to acknowledge FAPERJ and CNPq for grants used to support this research. We also would like to thank Dean of Extension of Federal University of Rio Grande do Norte, the National Institute of Nuclear Engineering of the State of Rio de Janeiro for their support and partnership in the execution of this study, and the inhabitants of Mãe Luíza community for accepting and be available to participate in the research.

REFERENCES

CARVALHO, L., et al. (2013). Risco, desastre e resiliência – um desafio para a cidade da Amadora. IX Congresso da Geografia Portuguesa. Universidade de Évora.

CARVALHO, R. J. M. (2012). ERGOPOLIS: an ergonomics approach applied to a city. Work 41 6071-6078. ISSN: 1051-9815

CHAN, E. (2013). Bottom-up disaster resilience. Nature Geoscience, V. 6. Available in : www.nature.com/naturegeoscience

DARSES, F. REUZEAU, F. (2007). Participação dos Usuários na Concepção dos Sistemas e Dispositivos de Trabalho. Cap. 24, p. 343; In FALZON, P. Ed. Ergonomia. Editora Blucher.

Hollnagel, E., (2012). FRAM, the functional resonance analysis method: modeling complex socio-technical system. Ashgate,UK.

KULIG, Edge, & Joyce (2008). Understanding Community Resiliency in Rural Communities Through Multimethod Research Journal of Rural and Community Development 3, 3 (2008) 77–94 7

ISDR (2002). International Strategy for Disaster Risk Reduction. Report on the Decade for Disaster Risk Reduction.

QUARANTELLI, E.L. (1988). Disaster studies: An analysis of the social historical factors affecting the development of research in the area. International Journal of Mass Emergencies and Disasters, 5: 285-31

RODRIGUES, Teresa. (2010). Notes, News and Reviews. The International Strategy for Disaster Reduction. RISK - Portuguese Association of Risk, Safety and Security. Territoruin.

SCHMITZ, W. (2000). Driving Macroergonomics Home: A Community Ergonomics Conceptualization. *In* Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2000.

UNISDR (2007). http://www.unisdr.org/we/inform/terminology. Assessed at: 20/03/2015.

UNISDR, (2015). The United Nations Office for Disaster Risk Reduction. Avaliable in: http://www.unisdr.org/.

UNISDR(2012., Como Construir Cidades Mais Resilientes: Um Guia para Gestores Públicos Locais (2005 – 2015).

WOODS, D. D.; Hollnagel, E.(2006). Prologue: Resilience Engineering Concepts *in* Hollnagel, E. Woods, D. Leveson, N. Eds. Resilience Engineering Concepts and Precepts. UK Ashgate.

OVERVIEW OF CHALLENGES IN RESILIENCE ENGINEERING: A CONSULTATION ON THE FINDINGS OF THE LLOYD'S REGISTER FOUNDATION INTERNATIONAL WORKSHOP ON RESILIENCE ENGINEERING

Michael Bruno
Dean, School of Engineering & Science Stevens Institute of Technology
Castle Point on Hudson, Hoboken, New Jersey, 07030 USA
mbruno@stevens.edu www.stevens.edu
Ruth Boumphrey Head of Research Grants Lloyd's Register Foundation
71 Fenchurch Street, London EC3M 4BS, UK ruth.boumphrey@lrfoundation.org.uk www.lrfoundation.org.uk

Abstract

Recent natural and man-made disruptions around the globe have over the last decade spurred widespread interest in the improvement of community resilience. We here define "community" in general terms ranging from local neighborhoods to a nation (and beyond). Resilience as articulated in this manner is not easily quantified, standardized, measured, and modeled. Success will require the integration of seemingly disparate disciplines (e.g., behavioral psychology and software engineering), the involvement of widely diverse stakeholders (e.g., power authorities and the insurance industry), and perhaps even the invention of new fields of study (e.g., measurement science). The Lloyd's Register Foundation is a charity helping to protect life and property by supporting engineering-related education, public engagement and the application of research. LRF has identified Resilience Engineering as a priority research theme in which it plans to make investments. Given the vast scope of this domain, and the numerous activities in the area already planned or underway around the world, it is essential that a careful assessment be conducted with the aim of identifying:

- The applications of Resilience Engineering to sectors of relevance to the LRF;
- The gaps in our ability to understand, communicate, and improve resilience in these sectors.

In partnership with LRF, Stevens Institute of Technology will host an international workshop on April 15- 17, 2015 with the aim of providing answers to the questions outlined above.

The workshop will include the participation of experts from around the world representing a diverse array of disciplines relevant to resiliency. The participants will produce a draft report summarizing the findings from the workshop presentations and discussions, and identifying the research areas in which LRF might consider making investments to most effectively further community resilience.

CROSS DOMAIN EXPERIENCE

ENGINEERING STRATEGY: A HOLISTIC VIEW ON THE DESIGN OF COMPLEX SYSTEMS

Eric A. van Kleef
Van Kleef Consultancy
Geulwijk 16, 3831 LM Leusden, The Netherlands
eric@vankleefconsultancy.nl

Abstract

Adaptation can be seen as an evolutionary process. Biological studies show that variation; retention and selection are enough ingredients for a system to drift in an amoral and unintentional way. The same mechanism works with organizations and complex systems. Human behavior shows variations from the best practice, unprofitable variations are wiped out, and the most profitable variations are retained in the new best practices. The variations that have the largest probability to be retained in best practices determine the adaptation or drift of the system.

Management to prevent systemic accidents often tries to control variation. People are pushed toward compliance with best practices. However, controlling variation without controlling drift will only postpone systemic accidents. Moreover, drift is also necessary to adapt to a changing environment. The most promising approach seems to get better grip on the mechanism of selecting variations for best practices.

The paper addresses the mechanism behind design and adaptation of complex dynamic systems. It elaborates on the conflict between diminishing variation in order to prevent accidents and the necessity of variation in order to adapt to changing environments. A possible way is shown to enhance the ability to adapt without jeopardizing safety.

1 INTRODUCTION

Ashby (1957) formally defined the dynamics of systems. He described a system by its state. In deterministic systems, the current state determines the state after one transformation. The consequence is, that all future states are determined from the first state, or starting condition. Ashby called the set of future states belonging to one starting condition a trajectory. He observed that the state space could be divided in several subspaces, whose boundaries where not crossed by any trajectory. He called these subspaces basins. In each basin the system tends to an equilibrium state, what he called an attractor. Attractors can be stable states, in which the system is stationary, and periodical states, that consist of a number of states that follow each other periodically. Later research (Lorentz, 1963; Ruelle & Takens, 1971) showed that even a third kind of attractor is possible, a so called 'strange attractor', that consists of a seemingly random sequence of states within a basin. It is impossible for a deterministic system to leave a basin as long as the environment of the system remains unchanged.

Changes in the system's environment shift the boundaries of the basins. In fact, it is even possible, that new basins are formed or old ones disappear (De Souza & Rodrigues, 2002). During such an environmental change, the system can get into a different basin, if the change in the environment happens so quickly that the system can not adapt. If a bowl with a ball resting at the bottom is moved slowly, the ball will remain near the lowest point of the bowl. If the bowl is moved suddenly, the ball doesn't have the time to adapt and can jump out of the bowl.

2 COMPLEXITY

If the number of components increase, the complexity increases. Weaver (1948) called this kind of complexity unorganized complexity. Modern literature commonly refers to this kind of systems as complicated (Hertogh & Westerveld, 2010).

Some systems possess such complexity that humans can not model them as a deterministic system. Then it is perfectly adaquate to describe them stochastically on a higher level of abstraction. In stochastical systems, the next state is only partly determined by the last one, because a stochastical variation is added to it. This variation is independent from the history of the system. The boundaries between basins are no longer crisp; the system now has a probability to cross the boundary. Stochastical systems that are in their operational basin, have a probability of leaving that basin. Reliability is a measure for the probability that a system leaves its operational basin. Reliability belongs to the realm of stochastic models.

One characteristic of complex systems is, that they possess more than one, and sometimes a large numbers of basins. Also, in complex systems, relations tend to be non-linear. This means, that if the a change in the systems environment is made twice as big, the resulting change in the system state will no longer be twice as big as well. Lorentz (1963) showed that in non-linear systems small differences in starting conditions can have enormous consequences. These

two factors make those systems very intangible for humans observing them. Intangibility and human incapacity of understanding, however, is not the main characteristic of complexity. It is merely a result of the large number of basins and the non-linear behavior.

3 ADAPTATION IN BIOLOGY

The properties of the system may change over time. Examples of this are wear and tear of mechanical components, but also the adaptation and learning of human components. Adaptation takes place due to some internal incentives of components and their exposure to environmental conditions.

Socio-technological systems are not only dependent on external factors to get moving. Humans differ from technology in having emotions. Internal drives for adaptation are pride, greed, lazyness, and fear. Instead of these pejorative words, literature uses wordings like cost minimization, profit optimization (greed), finding easier ways to do things, optimal use of technology, tight plannings (lazyness), risk avoidance (fear). This changing in the system originating in internal factors can be seen as adaptation. Essentially, these factors are the same as identified by Rasmussen (1997). Several components of the system can adapt independent of each other. The overall system can change its properties thereby drifting into failure (Woods, 2003; Dekker, 2011).

Comparing adaptation in socio-technical systems, whether engineered or emerged, to biological evolution can give some additional insights to the phenomenon of adaptation. Let us first have a look into the evolutionary process in biology. Wallace (1870) and Darwin (1876) formulated this concept. Simply said, it means that individuals within one species show some genetic variation. Darwin and Wallace were the first ones to note that the variety in species could be explained from small variations in individuals that cumulated over time. Some individuals have larger chances of reproducing than others. The children of the reproducing individuals inherit the genetic variations from their parents. The variations that have the largest probability to be carried over to the next generation will prevail and become the starting point for the variations in the next generation. The logical consequence of this mechanism is that the set of variations withing the species changes in a way that variations with a greater chance of reproduction are more abundant in within the species. The resulting evolution process, although amoral and unintentional, produces species that are fittest for the environment they live in.

Therefore, in order to have evolution, three elements have to exist in the system: variation, retention and selection. Without variation, we have no alternatives for the selection to work on. Without retention, the variations cannot accumulate. The selection mechanism is simply a mechanism that makes the probability of being copied in the next generation of variations dependent on the emergent properties of the previous generation. It can be intentional, as is the case in dog breeding programs, or unintentional, as is the case in natural selection. Evolution does not require a goal for evolution, in fact evolution as we find it in nature can be understood without an hypothesis about a goal.

4 ADAPTATION IN SOCIO-TECHNICAL SYSTEMS

Every function in a complex system is executed with a certain variation (Hollnagel, 2012). This variation may be very small, as it is in automated processes, or large as it is in human actions. There is a striking resemblance between the way these variations can lead to adaptation and the way evolution results from genetic variation in biology. All three elements can be found in socio-technical systems. Variation is abundant in human performance, retention is found in experience, best practices and procedures. The selection mechanism consists of the copying of variations. Variations in performance that are percieved as more successful are copied or retained in best practices. Variations that are percieved as less successful are not copied. We do have some clues as how this selection works. People tend to keep variations that earn more money, cost less, take less time, are easier, or are safer. Essentially we have the incentives as identified by Rassmussen. As all three necessary elements of evolution are present, we may expect evolutionary processes.

The best practices in a system tend to differ more and more from the original. Around this best practice many variations occur. One of these variations may prove to be fatal, a systemic accident occurs (Dekker, 2011). It is impossible to determine whether the variation or the best practice is to blame for the accident. There is simply no way to determine whether the deviation of the best practice was too big or that the best practice was too dangerous because it didn't allow for variations that occur.

Systems will adapt until the combination of adaptation and variation will result in accidents. Accidents are a collateral damage of evolution. In nature, many individuals die while the species adapt, and many species become extinct during evolution. Evolution in nature has no ethical considerations. The evolutionary process is amoral and unintentional. It chooses the adaptations that enlarge the probability of reproduction without ethical considerations.

In fact, the same selection process takes place at the level of organizations. Few systems are complete monopolists. Most systems compete with other systems for scarce resources. A system that does not adapt will be wiped out by competition. This is why systems that do not allow variation will not survive in the long term. In our analogy with

biology, the organization can be seen as the species, while existing variation between individual occurrences of actions can be seen as the individuals. In biology, we find species with little genetic variation and species with large genetic variation. Species with little genetic variation are very sensible to environmental changes because they cannot adapt quickly enough. Genetic variation is considered a value because it makes the species resilient to enviromental changes.

Systems that have too much variation will finish because some fatal combination of variations occurs that is not compatible with the existance of the system. Systems with are successful in regulating the amount of variation, in such a way that they remain compatible with their existance and they will remain competitive at the same time, will ultimately survive. This is the sustained adaptability of Woods.

The organizations that exist today are the product of the selection in the past. We may assume that the existing organizations have been pretty successful in adapting to the environmental changes in the past, as is proved by their mere existance today. The question remains whether we as humans can outperform the natural selection that is already taking place. We have an ethical obligation to ensure that the variations will not jeopardize human safety.

We humans have a marking difference with nature in that we can reflect on our own adaptation. We are, however, still subject to the laws of natural selection. In the same way, humans in socio-technical systems are subject to the adaptation laws, but they can reflect on the way they select variations as successful. We have the possibility to determine the incentives in the organization that will determine how best practices are selected. Only trying to diminish variation will not contribute to sustained adaptation, but will lead to extinction.

As we humans have ethical objections against accidents. Two approaches exists to avoid accidents. One is to control variation and the other to control drift. Many organizations tend to control variation. In fact, the whole concept of ‘human error’ is based on the idea that humans should not variate from best practice. Variation, however, is an essential ingredient for adaptation. At the same time, controlling variation without controlling adaptation will prove ineffective. The adaptation is simply allowed to proceed a little further until an accident happens.

The other, and more promising approach is to control drift. The system should not be allowed to adapt that much, that accidents will start to occur. We can try to continuously monitor the safety of the system and to intervene as soon as safety is jeopardized. But the most promising approach seems to be to have a closer look at the mechanism of selection. Which varieties are perceived as successful and allowed to be copied into best practices. Are the variations only selected by cost and time? Are variations selected on benefit for one department or also on benefit of the whole organization? Our research efforts should be aimed at this selection mechanism.

These internal adaptations of the system are to be well distinguished from the stochastical variations mentioned above. While stochastical variations are independent from each other in time, adaptations are systematic in character. Technological aging changes the parameters of the system as a function of time. Human adaptations are dependent on incentives and exposure. The system has a memory for things that happened in the past, the system ‘learns’.

5 RESILIENCE

Resilience can be better understood if looked upon from a evolutionary point of view. When looking at systems of systems, these systems can be in competition for a common resource. Darwin (1876) called the changes that occur in those situations evolution. A selection mechanism is needed to wipe out some systems from the world. As Slobodkin (1964) says: ‘Evolution is like a game, but a distinctive one in which the only pay off is to stay in the game.’

Resilience is about ‘staying in the game’, about survival of the system. Systems can cease to exist because their essential variables (Ashby, 1957) are sub standard as in the case of a human who is left without oxigen, or a company that goes bankrupt. But systems can also cease to exist because they loose the competition and are wiped out by selection. When talking about resilience, it is necessary to denote the evolutionary context of the system.

Systems whose essential variables are not compatible with survival, can simply be wiped out, like the human without oxygen. They can also get a sufficiently large disadvantage to loose competition with other systems.

In the latter case, the non resilient system is replaced by a completely new system, that was more able to survive than the old one. We could call such a complete replacement of one system with another a transition. In technology we often see that two completely different concepts are competing and that a disturbance in the old system gives the new one a great advantage in an evolutionary sense, thereby causing a transition to a new technology. Resilience of a system can thus be understood as the ability to maintain its competitive power in case of a disturbance. It is difficult to see what resilience means if no alternative is present; a monopolist will remain in power anyway. A strong competition puts the systems under pressure of losing their resilience.

As evolution knows the variation of individual behavior, the adaptation of species and the extinction and replacement by newer species, so does technology know variation within a mission, adaptation within a system and transitions where systems are replaced by new ones. Transitions are in the realm of evolution.

As stability relates to different basins, so does resilience relate to transitions between different systems. Lack of stability makes a system to transit to another basin, lack of resilience induces a transition to new system.

In the operational basin, the operator's behavior will be aimed at performance of the system. Near the edges of operational basin, safety will be the dominant factor. Once in a non-operational basin, operation's actions will be aimed at survival. Safety and resilience are not contradictory notions. They are indeed properties that have to be used together (van Kleef & Stoop, 2014).

6 CONTROLLING THE DESIGN OF COMPLEX SYSTEMS

Design processes are itself adaptable systems. They exist of a draft design and the designers, adapting themselves to the requirements under an incentive, most of the time some form of cost optimization.

If two designers have to self coordinate, they have to make sacrifices. Making sacrifices is only profitable, if making the sacrifice and thereby reaching a solution contributes more to the aim of the designer than reaching a deadlock. But if a deadlock is reached, the only way to get the flow back again is to make it more profitable to make sacrifices.

Ashby (1957) concentrates on systems that are controlled from outside. One of his observations was the law of requisite variety, stating that the variety in the dominant, controlling system has to exceed the possible variety of the controlled system. The consequence of this law is that controlling a complex system is practically impossible, because we need a very complex controller for this. An illustration from this idea can be found in the military. As armies bevcame more and more complex, the command and control structure grew. The last modern armies that were controlled, were the Brittish army in WO I, and the American army in Vietnam. Both armies proved not very successful (van Creveld, 1985).

This makes the decision not trying to control the development of new large complex infrastructure systems plausible. In fact, it would be impossible to control this design in every possible way from a central organization.

In the eightteenth and nineteenth century it was quit normal to look upon humans as variable in their acts. Emphasis in safety was put on values as 'good seamanship'. Scientific reductionism tried to explain everything from the properties of parts. Taylorism at the dawn of the twentieth century brought the legacy of reducing humans even further and depriving them of the essence of humanity, their spirit.

Complex systems have properties that can not be reduced to the properties of their composing elements. A reductionistic view on these systems will not be enough to describe them. The commissioner is interested in the properties of the system as a whole and not in the properties of the components. The emergent properties are too important to be left emerging. The different systems all have their own incentives. They can adapt in different directions. During this adaptation they influence each other in a highly complex way. There is no guarantee that these adapted systems still have the right properties together.

The growing complexity of the systems we build, makes this paradigm more difficult to maintain. In a lot of disciplines, scientific reductionism still hampers new paradigms about safety and resilience. We need a return to holism as an additional paradigm (van Kleef & Stoop, 2014). We have reached a point in history where we are no longer designing systems, but systems of systems, that are closely coupled. These systems of systems have such a large complexity that it is no longer feasable to control them completely. The commissioner has, however, still an aim to get a system that has some preset properties. It is therefor not enough to manage the process and just to wait and see what will happen, and only looking upon the process.

In the design of infrastructural systems, a stratification in control can be seen. The top level decisions are political ones. Westerheijden (1988) showed, that these decisions are made almost without techological knowledge. The next centralized level, what could be called a engineering-strategic level, seems however to be missing. Different actors, each designing one system in a system of systems, can not be relied upon to self-coordinate their designs. In one form or another, the functionalities of the sub systems and their interrelations have to be looked upon in a holistic way, in order to control the emergent properties, that are of imminent importance to the commissioner. There seems to be a need of an engineering-strategic level. In former days, chief engineers could fulfil this function. The increased complexity of the systems co-incided with a decrease of high-level technological knowledge in commissioning organizations. Also the tools that are needed at a engineering-strategic level are missing.

Designing with a fear and greed objective under technological constraints as is frequently done now, faces us with the problem that these technological constraints has to be such, that they guarantee technologically sound solutions. If these technological constraints take the form of 'comply with standards', or 'comply with law', we are using legal formulations as a technological specification. The combinations do not guarantee resilient or sometimes even operational solutions. Making technological designs on a strategic level, using functional analysis, enables us to add specific constraints to the standards. It will even enable us, to make strategic decisions about where to use 'greed and fear' optimizations and where to use technological optimizations. Tools for the engineering-strategic level of design are still in the first stege of development. Functional analysis seems to be a promising approach.In this way, functional analysis is in no way replacing old methods, but is complementing them, enabling technology to retake its central

position in complex design problems. This approach may be a seen as a first attempt to address the problem of sustained adaptability (Woods, 2014) during the design stage.

REFERENCES

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority* (2nd ed.). Washington, DC: CCRP. Retrieved from www.carlile.army.mil

Alberts, D. S., & Hayes, R. E. (1995). *Command Arrangements for Peace Operations.* Washington, DC: CCRP. Retrieved from http://www.dodccrp-test.org

Alberts, D. S., & Hayes, R. E. (2006). *Understanding Command and Control.* Washington, DC: CCRP. Retrieved from http://www.dodccrp-test.org

Ashby, R. (1957). *An Introduction to Cybernetics* (2nd ed.). London: Chapman & Hall. Retrieved from pespmc1.vub.ac.be

Darwin, C. (1876). *The origin of species by means of natural selection or the preservation of favoured races in the struggle for life.* London, England: Murray. Retrieved from http://darwin-online.org.uk/converted/pdf/1876_Origin_F401.pdf

De Souza, J. R., jr., & Rodrigues, M. L. (2002). An investigation into mechanisms of loss of safe basins in a 2 D.O.F. non-linear oscillator. *Journal of the Brazilean Society of Mechanical Sciences, 24*(2), 93-98. Retrieved from http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-73862002000200002

Dekker, S. (2011). *Drift Into Failure: From Hunting Broken Components to Understanding Complex Systems* (Adobe digital ed.). Farnham, England: Ashgate.

Hertogh, M., & Westerveld, E. (2010). *Playing With Complexity: Management and Organisation of Large Infrastructure Projects.* (Ph. D. thesis Erasmus University Rotterdam,The Netherlands). Available from http://www.netlipse.eu.

Hollnagel, E. (2012) *FRAM, the functional resonance analysis method: Modelling complex socio-technical systems.* Farnham, England: Ashgate.

Lorentz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences, 20*(2), 130-141. doi:http://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2

Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science, 27*(2/3), 183-213. Retrieved from http://www.ocw.nur.ac.rw/NR/rdonlyres/Aeronautics-and-Astronautics/16-358JSystem-SafetySpring2003/0E565A87-DFC1-4A54-B751-DF36BA2D6147/0/rasmussensafetyscience.pdf

Ruelle, D., & Takens, F. (1971). On the nature of turbulence. *Communications in Mathematical Physics, 20*(3), 167-192. doi:http://dx.doi.org/10.1007/bf01646553

Slobodkin, L. B. (1964). The strategy of evolution. *American Scientist, 52*, 342-357. Retrieved from http://www.jstor.org/stable/27839075

van Creveld, M. (1985). *Command in War.* Cambridge, MA: Harvard University Press.

van Kleef, E. A., & Stoop, J. A. (2014, 29-30 May). Reliable, Resilient: Towards a Dialectic Synthesis. Paper presented at *46th ESReDA Conference, Turino, Italy*.

Wallace, A. R. (1870). On the tendencies of varieties to depart indefinitely from the original type. In *Contributions on the theory of natural selection.* New York: MacMillan. Retrieved from https://archive.org/details/contributionstot00wall

Weaver, W. (1948) Science and complexity. *American Science 36*(4), 536-544. Retrieved from http://philoscience.unibe.ch/documents/uk/weaver1948.pdf.

Westerheijden, D. F. (1988). *Schuiven in de Oosterschelde.* [Slides in the Eastern Scheldt] (Ph. D. thesis University of Twente, The Netherlands).

Woods, D. D. (2003). *Creating Foresight: How Resilience Engineering can Transform NASA's Approach to Risky Decision Making.* (Testimony on The Future of NASA for Commitee on Commerce Science and Transportation, John McCain, Chair). Available from http://history.nasa.gov/columbia/Troxell/Columbia%20Web%20Site/Documents/Congress/Senate/OCTOBE~1/Dr.%20Woods.pdf.

Woods, D. D. (2014). *Velocity NY 2014 Keynote: The mystery of sustained adaptability*. Retrieved from http://www.youtube.com

MEALS AND INGREDIENTS: COPING WITH COMPOUND RESILIENCE STRATEGIES

Jonathan Day [1], Dominic Furniss [2], and George Buchanan [1]
[1] Centre for HCI Design, City University London, UK
[1] {Jonathan.Day.2 & George.Buchanan.1} @city.ac.uk
[2] UCLIC, University College London, UK
[2] D.Furniss@ucl.ac.uk

Abstract

Human performance constitutes a crucial contributor to the resilience of sociotechnical systems. The actions and behaviours performed by actors can themselves be deemed resilient, when individuals deploy resilience strategies. We build upon existing work which has sought to provide a vocabulary for different resilience strategies. The key concept we explore in this paper is 'compound strategies'- where individuals combine multiple motivations and behavioural mechanisms in their pursuit of heightened resilience. We draw an analogy between the role of recipes in combining ingredients to produce a meal, and the manner in which underpinning mechanisms are synthesized to compose a resilience strategy. We further discuss and define compound resilience strategies and demonstrate some of the challenges we have faced in their investigation through real-world examples. We subsequently propose a conceptual framework for deconstructing and analysing compound resilience strategies, and share implications for researchers in this field.

1 INTRODUCTION

As has been recognised in the literature addressing resilience engineering, human performance can be conceptualised not only as an inherent risk or weakness in sociotechnical systems (traditionally a prevailing view) but also as a potential source for maintaining system performance and increasing resilience. This move away from focusing exclusively upon negative aspects of performance (errors, risks, frailties etc.) but towards also recognising the value of opportunities to proactively maintain or manage performance, at an individual level, echoes the more broad distinction which Hollnagel draws between *Safety I* and *Safety II* (Hollnagel, 2013). It is this propensity, for individuals to proactively recognise and respond to challenges and threats in order to manage or maintain performance, that this work aims to further explore.

1.1 Resilience as a Behavioural Phenomena

One feature of the current literature on resilience engineering is a tendency to consider the topic of resilience in the context of wider systems, processes and organisations. In so doing, we are able to ascertain a broad and holistic account of resilience, which can be extended and transferred across domains, tasks and settings. At the same time, however, a key challenge arises in terms of establishing how to instigate change or apply resilience-related insights in a tangible, effective sense. Focusing on the behavioural phenomena of human actors at the 'sharp-end' within sociotechnical systems represents one clear avenue through which such change may be realised, and affords us a more concrete way to deliver the application of our understanding into resilience.

The work presented here focuses on what we refer to as *resilience strategies*. These comprise certain tactics and behaviours which, when utilised by actors within a system or by individuals more generally, make a positive contribution to safety, efficiency and overall performance. Such strategies may be both proactive and reactive, and address not only safety critical work but also more everyday challenges across all manner of tasks.

1.2 Existing Work into Resilience Strategies

In common with resilience in general, one unfortunate feature of the topic of resilience strategies is that we lack a history of targeted investigation of the concept. Investigations instead have scrutinised adverse events, instances of failure, and recognised or identified threats and challenges. However, where individuals or operators deploy strategies that have had a positive effect on the outcome of a sociotechnical system, this is often overlooked. The focus on tracing failure cases leads to the absence of a report when threats are avoided. Thus, successful action goes unreported. Such work is consequently sublimated into normal or routine practice without remark, and can be difficult to identify and extract for study. This presents a major barrier in investigating all forms of resilience.

As a result, the literature that specifically addresses resilience strategies is fragmented and relatively embryonic. Where resilient episodes are recorded and discussed, they are often termed in a different way, or discussed within the context of a more established but narrowly-scoped topic. For example, work targeting cues (Altman & Trafton, 2004), checking (Patterson, Woods, Cook & Render, 2006), appropriation (Dix, 2007), dynamic task restructuring (Iqbal & Bailey, 2006) and other such topics are of relevance. There are also many anecdotal accounts of strategies and

behaviours that are discussed in other contexts, and neither labelled or conceived in terms of resilience (e.g. Randel & Johnson, 2007) despite their value to the study of the topic. This issue of semantics makes it difficult to obtain a complete picture of the variety of resilience strategies deployed by individuals.

Recently, targeted efforts have however been made to articulate and analyse the variety of resilience strategies observable across a range of contexts. This work aims to provide a holistic account of these strategies, and establish a vocabulary to facilitate discussion and investigation. Furniss, Back and Blandford (2012) present a seven-item categorisation scheme that can enable the analysis of instances of resilience, a contribution that builds on the repertoire component of their *Resilience Markers Framework* (Furniss et al. 2009).

1.3 Investigating the Diversity of Resilience Strategies

While the work of Furniss, Back and Blandford (2012) proved useful in articulating and describing a variety of types of strategies, limitations in the original investigation existed. With regards to the category descriptors presented, the authors acknowledged that some of the categories appeared overlapping and ambiguities were still present, suggesting refinements in terminology but also potentially in framing and coverage may be possible. Additionally, the dataset upon which the categories were derived suffered from limitations both in terms of breadth (49 instances across 5 contributors) and depth (owing to a 140-character limitation in composing entries, reflecting the use of twitter for data collection).

We sought to replicate this idea using an expanded dataset, in an effort to validate and develop the scheme. We analysed an extended pool of data from 6 studies incorporating multiple methods (ranging from self-report and survey data to observations from a lab study) resulting in a total of 120 resilience strategies from which a revised scheme was derived. One persistent source of complexity during this exercise however was the classification of complex, 'edge-case' examples. While many episodes could be classified with relative ease, others proved more challenging, dividing opinion within our inter-rater reliability analyses. Examining these led us to conceive the notion of compound strategies.

2 THE EMERGENCE AND INVESTIGATION OF COMPOUND STRATEGIES

One common pattern emerged from the further examination of the problematic cases encountered while using the existing categorisation scheme. In numerous cases, and despite refinements to the scheme, instances appeared to draw equally from multiple categories. Reflecting on this led us to reconceptualise the nature of our strategy episodes: rather than considering such instances to be individual, self-contained examples of resilience strategy use, we instead consider they can be compounds of multiple behavioural and motivational components. Taking this new approach, the 'problem' of assigning one episode to one category over another becomes redundant: instances can simultaneously reside in more than one category, if meaningfully deconstructed into their constituent components.

2.1 Examples of Compound Resilience Strategies

> *Finding an improvised post-it note, sellotaped to a parking payment machine, informing users which buttons to press and in which sequence to avoid a seemingly common error*

This episode, collected as part of our ongoing collection of such instances, describes a strategy which seemingly contains two important aspects: generating an improvised note, and ensuring it is displayed front-and-centre so as to provide the information clearly and in a timely manner to users. It could be said to simultaneously involve generating an artefact in the form of the instructions, but also has strong elements of cueing, and improvising the attachment of the note onto the machine.

> *When out and about, and needing to take a copy of a receipt or similar, I will take a photo on my mobile phone. As I regularly check my photos, this is quite reliable*

While this again appears a relatively simple episode, this challenged the categorisation scheme as it features multiple resilient qualities upon closer analysis. One resilience strategy noted in the scheme is the improvised appropriation of items- in this example, the camera is appropriated as a means to create a digital copy. However the strategy is also compatible with the descriptors *creating an artefact* and debatably, *adjusting a routine or behaviour*.

2.2 Compound Resilience Strategies: Meals and Ingredients

The identification of these compound strategies motivated us to reconceptualise the application of the scheme categories, adjusting their nature and purpose. Rather than mere labels or descriptors, we have enriched their role to become representations of the underlying mechanisms from which strategies are composed. The analogy of meals and ingredients (inspired by Woolwych et al, 2011) becomes a useful way to illustrate the concept. Our shift in perspective

represents a shift from considering strategy episodes as ingredients, instead to meals in their own right: products resulting from the synthesis of constituent ingredients that take the form of behavioural and motivational components.

3 A FRAMEWORK FOR THE DECONSTRUCTION OF COMPOUND STRATEGIES

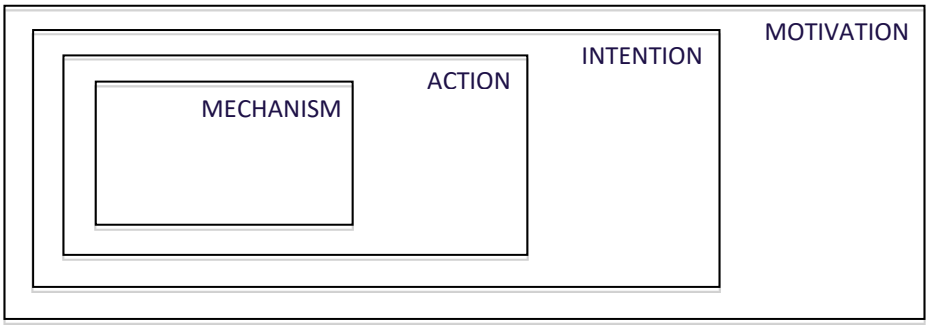


Figure 1. A framework for the deconstruction of compound resilience strategies. The framework presupposes the breaking down of complex, compound strategies into components at four levels: high-level motivations, intermediary goal-based intentions, observable and concrete actions, and resilience mechanisms (formerly the descriptors or category labels in the Furniss et al, 2012 scheme). This representation of the framework also reflects how motivations encapsulate intentions, which in turn encapsulate actions, encapsulating mechanisms

We propose a basic framework (represented in figure 1, above) to assist researchers and practitioners in analysing and making sense of compound resilience strategies by breaking them down into their components, or ingredients. Our approach is inspired by the GOMS approach to modelling human computer interaction (Card, Moran and Newall, 1983) which similarly deconstructs tasks into the motivations and mechanisms necessary for their completion. Our framework proposes the analysis of strategy episodes can be assisted by deconstructing them into four aspects at differing levels of granularity:

Motivations at the highest level represent the overarching broad goal that a strategy addresses. We conceptualise this in terms of risks and rewards, reflecting threats which impact the successful completion of a task or process, while opportunities to improve performance or efficiency. We posit strategies inherently address one of these two aspects.

Intentions represent context dependent, task-oriented goals that an individual intends for their strategy to address. Depending on the nature of the strategy and the threat it addresses, there may be more than one intention present in a strategy.

Actions represent the concrete, observable action that an individual/operator takes to achieve their intention(s). The actions available again reflect the context of a strategy (i.e. task and environment, resources/expertise/ability available to the operator etc.) Each intention generally has at least one corresponding action, however multiple actions may be used to resolve one intention. A single action may also address multiple intentions.

Mechanisms describe a set of prototypical mechanisms that underpin a strategy and describe how or why it works. Each action will correspond to at least one mechanism, however multiple mechanisms may be achieved in one action. These mechanisms are transferable across domains, tasks and settings, and constitute the reconceptualization of the category labels or descriptors in the Furniss et al (2012) categorisation

3.1 Applying the Framework to Instances of Resilience Strategy Use

To illustrate how the framework can assist with the analysis of accounts of compound strategies, we now deconstruct the two examples of previously presented in section 2.1.

Regarding the example of the improvised note on the parking machine, the motivation is the avoidance of an error, reducing the chance of a threat preventing the completion of the task (MO1). The intention can be divided into two goals, the primary being to generate supplimentary instructions to assist the user (I1) and a secondary or subgoal being to ensure this information is available when required (I2). The observable actions can thus be considered as composing the note (A1) which addresses I1, and sellotaping the note onto the device (A2) which addresses I2. In terms of mechanisms, based on the category descriptors derived from our expansion on the Furniss et al (2012) scheme, we identify *ME1 creating an artefact* (mapping to A1 in terms of producing an informational artefact), *ME2 creating a cue* (relating primarily to A2 in ensuring the prominent location of artefact, prompting users in their interaction) and *ME3 reinforcement* (reflecting the use of sellotape to provide additional security in keeping the note in place, addressing I2 and reflecting A2).

Regarding the second example, we see two motivations emerge: the broad goal of addressing the threat represented by data loss (MO1) and a secondary motivation of improving performance, by making the the file more easy and quick

to locate (MO2). In terms of intentions, the user in this case has an intention of generating backup versions (I1) and also distributing backups across multiple locations (I2). The observable action the user takes is simply to copy their file to multiple locations (A1), which addresses both intentions I1 and I2. In terms of mechanisms, again based on the aforementioned category descriptors, we identify *ME1: adjusting a procedure or behaviour* (in terms of incorporating additional task steps), *ME2: reinforcing an existing safety barrier* (where I2 reduces impact of lost backup), and *ME3: Managing resource availability* (addressing secondary motivation MO2).

4 DISCUSSION

The relative immaturity of the literature specifically addressing individuals' resilience strategies presents a challenge to structured and consistent analysis. All too frequently, interesting and insightful episodes and accounts of resilient behaviour are reported only anecdotally, if at all, which limits the value contributed by this potential resource. Recent efforts to provide an analytical foundation for investigating and discussing resilience strategies have proved problematic, due to the complex nature of some recorded instances of resilience, which seemingly combine multiple interrelated ingredients. The framework we propose here provides a means to unpack and deconstruct these compound strategy cases, enabling structured and in-depth analysis of the mechanisms and motivations that underpin such strategies. We move beyond looking at strategies as indivisible wholes to consider the ingredients upon which they're made (high level motivations, intentions and goals, observable actions and underpinning mechanisms) and recipes in terms of how they're put together (exploring the relationships between the ingredients).

At this point, we acknowledge however that this framework and the specification of the mechanisms are a work in progress, and may be subject to further revision or refinement. The 'motivation' component for example, while providing an framing device to situate an episode and elicit reflection on the nature of the threat or opportunity, may bring only limited insight, and in some cases result in increased ambiguity. We would however reiterate that the framework in its current form, as with the categorisation scheme before it, is first and foremost a tool to stimulate discussion, structure analysis and provoke further insight. It is not intended to be seen as a formal or rigorous apparatus, and some level of ambiguity in terms of identifying the ingredients or specifying the recipe is to be expected.

Despite this, we maintain that the framework plays a useful and as yet largely unaddressed role in facilitating the analysis of compound resilience strategies. In providing insight into resilience episodes observable across a broad range of contexts, we suggest this work assists not only analysis of domain-specific existing accounts of resilience, but potentially facilitates transfer of resilience strategy insight across domains. By deconstructing complex strategies and understanding why (motivations) and how (mechanisms) they work, one is in a stronger position to accommodate and manage the implementation of resilience strategies at the 'sharp-end' of interactions with future sociotechnical systems.

Acknowledgements

We gratefully acknowledge the support of the UK EPSRC grant [EP/G059063/1], *CHI+MED*. We also thank *Jonathan Back* for his contribution to the original and revised categorisation schemes, and *Katarzyna Stawarz* and *Atish Rajkomar* for contributing strategy episode data.

REFERENCES

Altman, E. M. & Trafton, J. G. (2004). Task Interruption: Resumption Lag and the Role of Cues. Proc. 26th Annual Conference of the Cognitive Science Society.

Card, S., Moran, T. P., & Newell, A. (1983). The Psychology of Human-Computer Interaction, Lawrence Erlbaum Associates, Hillsdale, NJ.

Dix, A. Designing for Appropriation. (2007). Proceedings for the British Computer Society's Annual Conference in HCI '07, 2, 28-30.

Furniss, D. Back, J., Blandford, A,. Hildebrandt, M. & Broberg, H. (2011). A Resilience Markers Framework for Small Teams. Reliability Engineering & System Safety, 96, 1.

Furniss, D., Back, J. & Blandford, A. (2012). Cognitive Resilience : Can we use Twitter to Make Strategies More Tangible? Proc. ECCE 2012, 96–99. ACM Press.

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

Iqbal, S. T. & Bailey, B. P. (2006). Leveraging Characteristics of Task Structure to Predict the Cost of Interruption. Proc. CHI 2006, 741-750. ACM Press.

Patterson, E. S., Woods, D. D., Cook, R. I., & Render, M. L. (2006). Collaborative cross-checking to enhance resilience. Cognition, Technology and Work. 9:155–62.

Randell, R. (2007). User adaptation of medical devices. Cognition, Technology and Work. 3163–170.

Woolwych, A., Hornbæk, K., Frøkjær, E. & Cockton, G. (2011). Ingredients and Meals Rather Than Recipes: A Proposal for Research That Does Not Treat Usability Evaluation Methods as Indivisible Wholes. International Journal of Human-Computer Interaction, 27:10, 940-970.

ON THE NATURE AND ROLE OF ORGANIZATIONAL DYNAMICS IN ADAPTIVE SAFETY

Lawrence J. Hettinger [1], John M. Flach[2] and Marvin J. Dainoff[1]
[1] Liberty Mutual Research Institute for Safety, 71 Frankland Road, Hopkinton, MA 01748 USA
[1] {Lawrence.Hettinger, Marvin.Dainoff}@libertymutual.com, +1 508 597-0297
[2] Wright State University, Department of Psychology, 3640 Colonel Glenn Highway, Dayton, OH 45435 USA
[2] John.Flach@wright.edu

Abstract

How can organizations maintain an effective posture of proactivity and adaptability with regard to safety in an increasingly complex, interconnected world in which change occurs at rates ranging from the gradual and quasi-predictable to the sudden and unexpected? In this paper we will present a general systems theoretic perspective on adaptive sociotechnical system behavior that emphasizes the foundational importance of coordinated, nested communication and feedback loops within organizations, supported by participatory design processes. Adaptability, we argue, can be considered to be an emergent characteristic of systems whose component interrelationships are characterized by clear channels of communication (specifying constraints on adaptive responses to safety risks) and feedback (providing "sharp end" perspectives on risks and requirements for effective response. We will primarily focus on issues related to organizational resilience and safety – i.e., worker safety, process safety and related public safety.

1 Organisational dynamics

We will focus on examining organizational issues involved in proactively promoting adaptive approaches to routine and catastrophic safety risks in a way that does not trivialize the complex nature of either the process or the nature of the risks to be addressed. Much of what has been attempted in the past has, in our opinion, fallen short precisely for this reason. To begin to address this issue, we believe there are two subordinate questions to examine: (1) how do we create and maintain a genuine and durable culture of proactivity with regard to safety, and (2) how can we effectively engage and codify expertise from across the organization (i.e., from the board room all the way to the factory floor) to guide the identification of potential risks and appropriate responses to mitigate these risks.

Addressing Culture – As is well-illustrated in Leveson's STAMP approach (Leveson, 2012), every organizational level within a work-based sociotechnical system (e.g., board room, CEO, senior management, middle management, floor supervisors, front-line workers, etc.) already plays a vital role in either promoting or retarding safety, whether they realize it or not. Each level of the hierarchy already responds directly to the constraints imposed upon it by the level to which it reports. To promote a culture of proactive safety that goes beyond banners and posters, each level must take seriously its role in providing appropriate safety constraints and expectations to the levels below it. Considerations regarding the *nature* and the *level of specificity* of these constraints are vital. Constraints (i.e., guidance, requirements, etc.) must exist, but to promote truly adaptive response they must not "over specify" or overly constrain the repertoire of adaptive behaviors afforded to individuals at the sharp end of the response. For example, over-reliance on "checklist approaches" to countering safety risk may inhibit the natural and more effective, adaptive responses of expert operators/workers and prove to be of little or no worth (or worse) in unusual or unanticipated situations.

However, the provision of effective constraints is only half of the equation. Constraints need to be continually re-examined and updated (or not) on the basis of reliable and accurate information or feedback from lower levels of the hierarchy up through the higher levels. Without this vital flow of information, constraints will become increasingly arbitrary and divorced from reality (e.g., Flach et al, in press). Anything that stifles or discourages this information flow reduces the capacity to adaptively response to safety risk.

Engage and Codify Expertise – A key element of information flow involves consistent, frequent, open and honest discussion about safety issues across all levels of the organizational hierarchy. These discussions should give priority to the authority of expertise (e.g., direct experience), rather than the authority of power (e.g., formal rank). Since the work environment and, therefore, safety are dynamic and complex, these discussions must occur frequently and must result in the formulation of updated safety constraints and feedback/communication approaches when appropriate.

The above represents a broad overview of two aspects of organizational dynamics that, in our opinion, directly impact the ability to adaptively respond to routine and non-routine safety risks. In our paper and presentation will we elaborate on principles of general systems theory and sociotechnical systems theory that support these assertions, as well as providing examples from the literature on and our experiences with accidents and mishaps – and successful adaptations to similar situations – as additional support.

REFERENCES

Flach, J.M., Carroll, J.S., Dainoff, M.J. and Hamilton, W.I. In press. Striving for safety:Communicating and deciding in sociotechnical systems, *Ergonomics.*

Leveson, N., 2012. Engineering a safer world. Cambridge, MA: MIT Press.

LEVERAGING RISK REGISTER INFORMATION FOR DEVELOPING RESILIENCE THROUGH RISK INTELLIGENCE

M.C. Leva [1] and N. Balfe [2]
[1,2] Centre for Innovative Human Systems, Trinity College Dublin, Dublin 2
[1] levac@tcd.ie 00353-1 896 2916
[2] balfen@tcd.ie 00353-1-896-3576

Abstract

Resilience can be defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel, 2011). Central to this definition is the core ability of an organization to understand, monitor and develop a risk intelligence capacity.

A risk database, or risk register, is a central tool for organisations to use to monitor and reduce risks, both those identified during initial safety assessments and those emerging during operations. The risk register should contain all analysed risks and should prioritise the areas that require managerial attention. When populated with information on each risk, including risk ranking, the risk register can be analysed to present the risk profile for different aspects of the organisation. When reviewed and updated over time, it can also be analysed to present trends within the risk profile and focus management attention on the highest risk activities or facilities. This research presents a concept of extending traditional risk registers through analysis of the information contained within them across an entire company (data-mining) to develop risk intelligence in order to support resilience.

The poster will present a concept of building risk intelligence to support resilience in safety critical industries using data from a risk register. The case study presented is from an electricity generation company, who have identified the need to better manage their safety and resilience information and have developed a comprehensive risk register containing information on technical, human, financial, environmental, and regulatory risks across the entire generation business. Electricity generation is an inherently high energy, multiple hazard industry that can potentially be harmful to life, health, assets, and the environment. The presence of this stored energy or hazardous substances, which when released can cause damage, can take many forms including, chemical, mechanical, thermal, electrical, etc. Process safety is concerned with preventing harm to people, the environment and the plant from this uncontrolled release of energy / hazardous substances through a combination of good engineering design / practices, asset and integrity management, and through good operation and maintenance practises (Hopkins, 2009). The company involved in this research operates a number of electricity generation stations and has an on-going programme composed of a multiple of projects to improve process safety.

In order to maintain safe operations, organisations must continuously review and monitor their risks. This means that the results of safety studies must be translated into a format that can be analysed, reviewed and acted upon, and new data about the level of risk continuously collected to keep the safety information up to date. A risk database, or risk register, is a central tool for organisations to use to monitor and reduce risks, both those identified during initial safety assessments and those emerging during operations (Whipple and Pitblado, 2010). The risk register should contain all analysed risks and should prioritise the areas that require managerial attention and typically contains information describing each risk, an assessment of the likelihood and consequences, a ranking according to a risk matrix, the risk owner, and information on the mitigations to be put in place (Filippin and Dreher, 2004). When populated with information on each risk, including risk ranking, the risk register can analysed to present the risk profile for different aspects of the organisation (Filippin and Dreher, 2004). When reviewed and updated over time, it can also be analysed to present trends within the risk profile and focus management attention on the highest risk activities or facilities (Whipple and Pitblado, 2010). In order to successfully develop a risk registry that provides an accurate level of risk within a process, there is a requirement for real time data on risk to be input into a risk registry.

The risk register developed as part of this research allows individual stations to document and monitor their

risks and to report upwards their priority risks (Balfe, Leva, McAleer & Rocke, 2014). However, the benefits are limited when confined to individual stations; this poster explores the potential to use the information captured for developing risk intelligence through data mining of the risk registers and sharing of risk information across sites. This approach can help develop overall resilience by facilitating learning across sites, improving the ability to anticipate risks, and monitoring risk profiles across the business. The poster will present the proposed approach, based on the existing risk registers.

REFERENCES

Balfe, N., Leva, M.C., McAleer, B. & Rocke, M. (2014). Safety Risk Registers: Challenges and Guidance. Chemical Engineering Transactions, 36, pp. 571-576.

Filippin K., Dreher L., 2004. Major hazard risk assessment for existing and new facilities. Process Safety Progress, 23, 4, 237 – 243.

Hollnagel, E. (2011). Prologue: The scope of Resilience Engineering and Epilogue: RAG – The Resilience Analysis Grid. In: Hollnagel E., Pariès, J., Woods, D.D., and Wreathall, J. (Eds.), Resilience Engineering in Practice: A Guidebook. Ashgate, Aldershot, UK

Hopkins A., 2009. Thinking about process safety indicators. Safety Science, 47, 4, 460-465.

Whipple T., Pitblado R., 2010. Applied risk-based process safety: A consolidated risk register and focus on risk communication. Process Safety Progress, 29, 1, 39-46.

ASSESSING RESILIENCE

CAN TEAM REFLECTION OF RAIL OPERATORS MAKE RESILIENCE-RELATED KNOWLEDGE EXPLICIT? - AN OBSERVATIONAL STUDY DESIGN

Willy Siegel1 and Jan Maarten Schraagen1,2
1University of Twente/BMS/CPE, P.O. Box 217, 7500 AE Enschede, Netherlands
A.W.Siegel@UTwente.nl ; J.M.C.Schraagen@UTwente.nl
2TNO Earth, Life, and Social Sciences, P.O. Box 23, 3769 ZG Soesterberg, Netherlands
jan_maarten.schraagen@tno.nl

Abstract

The essential resilience capabilities – monitoring, responding, learning and anticipating - have all in common the need for relevant signals and the ability to transform them into action. However, this transformation is often lacking as seen from accident analyses revealing disturbances that are either not noted or ignored in the process leading up to the undesired result. This paper proposes to focus on signals occurring because of movements from and to system boundaries and use them for team reflection. The reflection is expected to make implicit knowledge explicit, being a first step of the needed transformation to action. An observational study is designed at a rail control post where rail signal operators reflect at the end of their shift. They reflect on the punctuality boundary through an on-line application, called the Resiliencer-punctuality. The application presents delay-development of trains, during a shift, with respect to a previous chosen period. Furthermore it provides search instruments to find specific trains of interest stimulating the reflection. A verbal analysis method is used to analyze the reflection discussion and to show a relation to resilience through learning and anticipating intentions. In addition we seek for repetitive elements in different cases to prove the learning potential. The observation designed should support the hypothesis that team reflection, on movements towards boundaries, increases resilience of the rail socio-technical system.

1 INTRODUCTION

Resilience engineering researches, among other aspects, the ability of a socio-technical system to reorganize and adapt to the unexpected and unforeseen (Hollnagel, Woods, & Leveson, 2006). Hollnagel (2009) theorizes that a sociotechnical resilience system needs four essential capabilities: responding, monitoring, learning and anticipating. These capabilities differ in moment and scope – actual, critical, factual and potential – but have in common the need for 1) relevant signals and 2) the ability to transform them into action. This transformation is often lacking as seen from accident analyses revealing disturbances that are either not noted or ignored, leading up to the undesired outcome (Hall, 2003; Stanton & Walker, 2011). The sharp end can play an important role in this transformation. Cowley & Borys (2014) describe an organizational elasticity model with competent and knowledgeable workers at the sharp end to respond to drifts of performed work (Dekker, 2011; Hollnagel, 2008; Weick & Sutcliffe, 2007). Bracco, Piccinno, & Dorigatti (2014) go further by presenting nine steps to progress from the individual at the sharp end to the organization at the blunt end. However, it is not clear from the studies described above where the signals are identified and how they are transformed into explicit knowledge the organization can act upon. Signals appear throughout normal processes, having a large variability and are not necessarily related to the resilience of the system causing a large efficiency-thoroughness-trade-off (Hollnagel, 2009a). In an earlier study (Siegel & Schraagen, 2014b), we proposed to focus on signals related to the system boundaries to reveal resilience changes. Focusing on these resilience-related signals reduces the signal trade-off effort but still needs a process to turn them into resilient behavior - learning and anticipating. In this paper, we suggest to use team reflection to increase the amount of explicit knowledge, relevant to system resilience, enabling learning and anticipation. Team reflection (Ellis, Carette, Anseel, & Lievens, 2014; Reymen, 2003; Schippers, Den Hartog, & Koopman, 2007; Schippers, Edmondson, & West, 2014; West, 2000; Wiedow & Konradt, 2010), includes behaviors such as questioning, analysis, making use of knowledge explicitly, reviewing past events with self-awareness, and coming to terms over time with a new awareness (West, 2000). Team reflection, in a loop with planning and action, is used in a broader reflexive process (West, 2000) where team members collectively reflect upon the team's objectives, strategies, and processes. However, the team reflection proposed here goes beyond the team's span of control, which is located at the sharp end, knowing details not seen by the rest of the organization. The question arises whether team reflection exposes knowledge beyond the responsibility of the team and whether it adds to the existing explicit knowledge. Thus, the main aim of this paper is to develop theory and method, and design an observational study in a rail system environment to verify the effectiveness of the proposed method. In the next section, we describe the theory and method for use in the operational environment. Next, we describe the rail environment of the study including proposed processes. We end with a discussion on the expected results.

2 METHOD

We describe at first the setting to understand the context of the methods. A Dutch rail-post responsible for the area North and West of Amsterdam with about fifty rail stations and thousand daily train trajectories. The work, performed 24/7, assigned to rail signalers during the day across four workstations. The rail signalers have to monitor the system planning and execution. During disruptions, they adjust the planning, manually direct the system and follow safety procedures and protocols including communication with train drivers and other personnel. They enter information about every train delay of more than three minutes through a dedicated application on the cause of the delay. This is the only place where they capture their knowledge about the system. The rail signalers perform their tasks and go home after their shift without any organized discussion about their work. Due to large disruptions they may be approached for questioning. The team reflection method of the rail signalers at the end of their shift is a new activity described in the next subsection. The following subsection describes the method used in the reflection-tooling and the last subsection describes the analysis method used to classify verbal expressions during the reflection.

2.1 Team reflection of rail signal operators at the end of their shift

The team mentioned in this paper, is a group of rail signal operators working together during a shift at a rail control post. Team reflection has mainly been investigated with respect to the performance of the team itself. West (2000) defines the team reflection subject as the group's objectives, strategies (e.g., decision making) and processes (e.g., communication). The results of such a reflection can be fed back into the planning and action/adaptation loop to improve team performance such as their information processing (Schippers et al., 2014). However, in our case the objective of reflection is to transform implicit to explicit knowledge, at the sharp end, relevant to the resilience state of a socio-technical system. This knowledge goes beyond the direct responsibility of the team. Implicit knowledge is tacit knowledge, a form of private knowledge that is treated as "informal," and even, in a sense, "unconscious" knowledge (Day, 2005; Polanyi, 1969), that can be transformed to explicit knowledge (Frappaolo, 2008). We are interested in the implicit knowledge, relevant to system resilience, acquired throughout the regular work of the signalers. Resilience is about the behavior of the socio-technical system (STS) when it approaches and passes its boundaries (Siegel & Schraagen, 2014a; Woods, 2006). We assume that resilience related knowledge is released when the subject of team reflection is the movements towards and from those boundaries. We depict the proposed in figure 1. The signal operators interact individually with the rail STS, where they are part of as well. Throughout the interaction they gain individual implicit knowledge on the rail STS, which is partially made explicit through data entry by the signalers themselves into the system. Through the reflection they exchange some of their implicit knowledge, causing it to become explicit.

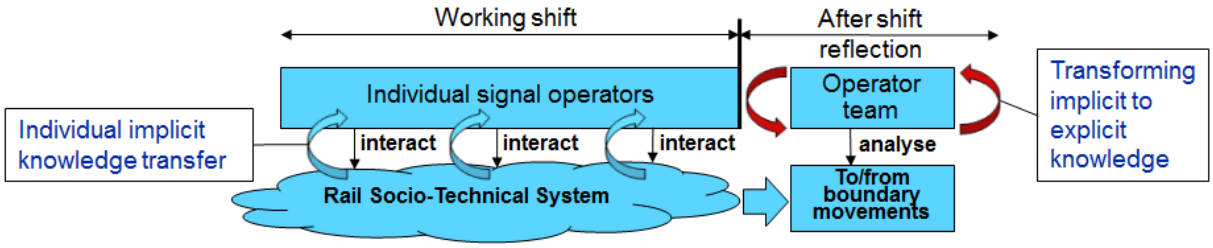


Figure 2 After shift reflection

2.2 Movements towards and from the performance (punctuality) boundary

In order to motivate the team reflection on topics related to resilience, we suggest to reflect on movements of the Operating System (OS) towards and from the boundaries as described previously (Siegel & Schraagen, 2014a, 2014b). In this paper, we focus only on the performance boundary and particularly punctuality. Performance in the rail sector is a combination of punctuality and capacity. In the short term only punctuality plays a role since capacity is nearly constant through its year planning. Punctuality of rail operations is well defined as the difference between planned (i.e. according to the latest published timetable) and actual moments of arrival or departure from a specific station (Goverde, 2005; Hansen, 2010). However in our case, we deal with many stations in a large area, many trains, different routes and shift periods, which need an extended punctuality definition to distinguish well between all these ingredients. This definition is the basis for the presentation and analysis during reflection. The context is a control area A and m stations S_j, j=1, …, m. In this area are n_A trains, T_i i=1,…, n_A, driving during de shift period between t_{shift}^{start} and t_{shift}^{end}. Train T_i has at station S_j a punctuality of $P_{i,j} = t_{i,j}^{act,dep/arr} - t_{i,j}^{plan,dep/arr}$ being positive

when the train is delayed. Where $t_{i,j}^{act,dep/arr}$ is the *actual* moment of arrival (arr) or departure (dep) of train T_i at station S_j and $t_{i,j}^{plan,dep/arr}$ is the *planned* moment. The train T_i has a route starting at station S_{Bj} and ending at station S_{Ej} where $S_{\square j}, S_{\square j} \in \{S_j, j = 1, \dots, \square\} \in \square$. The punctuality of train T_i at the start of its route in area A (station S_{Bj}) is: $P_{i,\square j} = t_{i,\square j}^{act,dep} - t_{i,Bj}^{plan,dep}$ and at the end of his route (station S_{Ej}) $P_{i,\square j} = t_{i,\square j}^{act,arr} - t_{i,\square j}^{plan,arr}$. A train, in this context, is defined as delayed when $(P_{i,Bj}\ or\ P_{i,Ej}) \geq t_d$, where t_d is a time duration set by de rail sector. In our case $t_d = 3$ min. This definition causes delays of train T_i *within* its trajectory at area A not be accounted as a delay.

Team reflection needs an indication on the performance of the trains within area A. We have chosen to calculate the punctuality increase of delayed trains during the shift. We present its relation to the same parameter during a reference period, which is the last week, month or year.

The increased punctuality of train T_i in area A is $\Delta_{\square} P_i = P_{i,Ej} - P_{i,Bj}$. The average increased punctuality of delayed trains T_i in area A during shift period between t_{shift}^{start} and t_{shift}^{end} is $\overline{\Delta_{\square} P}_{shift} = \frac{1}{n}\sum_{i=1}^{n} \Delta_A P_{i,shift}$ where n is the number of delayed trains driving in area A within the shift interval $t_{shift}^{start} \leq t_{i,Bj}^{act,dep}$ *or* $t_{i,Ej}^{act,arr} \leq t_{shift}^{end}$ causing trains, crossing the shift boundary, counted in both shifts. The average increased-punctuality of delayed trains in area A during a reference period of shifts is $\overline{\Delta_A P}_{ref}$.

Movements towards the punctuality boundary are identified through the relation between $\overline{\Delta_A P}_{shift}$ and $\overline{\Delta_A P}_{ref}$. When the first is larger than we talk about, a movement occurs towards the boundary, otherwise the movement is away from the boundary.

We have transformed the above into an application called the Resiliencer-punctuality (fig.2). The application has two main modes: Live and Analysis. Live mode presents in real-time the comparison between $\overline{\Delta_A P}_{shift}$ and $\overline{\Delta_A P}_{ref}$. Analysis mode freezes the live data and allows searches for particular trains and punctuality increase. The results are split in passenger and freight trains, since both have a different characteristic concerning time delays. Passenger trains are tightly coupled to the on-line published time-table, while freight deviates much easier and has a lower punctuality priority. We have split the controlled area into four main trajectories. This helps to understand the results of the whole area. On the right hand side of the live mode display are the four trajectories. In the analysis mode we integrate search functions to focus on a particular train of interest. We present a graph of its trajectory with its delays (see lower right window in the analysis mode display).

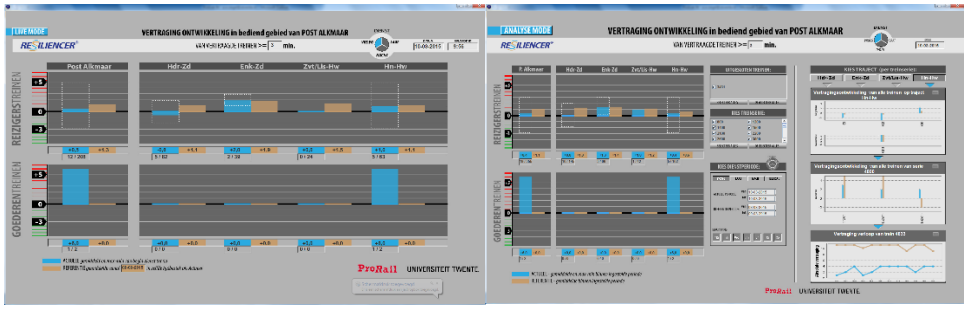


Figure 3 The Resiliencer-punctuality in live mode (left) and analysis mode (right)

2.3 Verbal analysis

To analyze implicit to explicit knowledge transformation during team reflection, we use the verbal analysis method. This method quantifies subjective or qualitative coding of verbal utterance contents (Chi, 1997). In contrast with the verbal protocol analysis (Ericsson & Simon, 1993), which focuses on capturing the process of problem solving to gain knowledge, the verbal analysis focuses on capturing the representation the solver has. In our case, there is no direct problem solving, but knowledge is presented by the participants throughout the reflection, which is shared by the team and needs a methodology to be captured. To uncover what a participant knows and shares with a colleague needs analysis of the verbal utterances. We propose the following steps to achieve a set of propositions, along with a procedure to organize the verbal content.

1. Reducing the protocols

The rail operations are organised around train numbers, which are uniquely defined during a day by its route and order of appearance on the route. These train numbers, which are central in the Resiliencer-punctuality as well, are taken as the definition of discussion cases. In all discussions, we assume an initial or leading train number, which we will use to split the discussion in cases and rank them in order of discussion length. The analysis will be concentrated on the longest discussion cases, assuming most knowledge transfer, thus most interesting for this research.

2. Segmenting the cases into semantic features, such as ideas, argument chains, or topics of discussion.

   This approach of semantics was also used by Chi (1997) and preferred over the non-content segmentation unit of a sentence, or a part of it. Because of two reasons: 1) an idea might need several sentences to convey and 2) the same idea might be repeated several times and should be recognized and treated as such. This content segmentation has a subjective bias and should therefore be segmented and compared to a second researcher as done for the coding of these segmentations.

3. Coding of the segments

   The segments are coded by at least two coders and compared to each other. The following coding scheme will be used:

   - Type of segment content: 1) Fact ; 2) Reasoning {+ Depth of reasoning}; 3) Suggestion ; 4) Opinion; 5) None of the above
   - Coding used in the Dutch reporting system for allocating delays (relevant for comparison):
     - Transporter (train operator): 1) Rolling stock; 2) Personnel; 3) commercial process; 4) Train knock-on delays
     - Infrastructure operator: 1) Civil engineering; 2) Defect Infrastructure; 3) Traffic management
     - Third parties: 1) Weather; 2) (near) Collision; 3) Strike
   - Knowledge within span of team-control: Yes/No

The analysis based upon the above coding will result in: 1) relation diagram of knowledge segments and 2) percentage of knowledge beyond the span of team control. The relation of knowledge segments will show the depth of reasoning, which is a type of learning (Felder & Henriques, 1995). The suggestions are a first step of anticipation. Learning and anticipation are both resilience cornerstones (Hollnagel, 2009b).

3 OBSERVATIONAL STUDY DESIGN

The study design at the Dutch rail-post described above, is about the introduction of team reflection (figure 3 in the top-center). At the end of the rail signal operators' duty (figure 3 in the center) they will discuss de- and increased delays within their controlled area. The will use for that the Resiliencer-punctuality (figure 3 left side). The application has been configured for the specific rail-post. It presents in live mode the punctuality status and provides in analysis mode the ability to search for logistic details (i.e. the delay progress of a specific train). The post-area has been split up into four main trajectories covering all stations and each trajectory is controlled by two workstations. This causes at least two rail signalers to relate to the results of a main trajectory. The results of the four trajectories are combined into results of the whole post during a shift.

The four rail signalers on duty will stop their work an hour earlier, during the observational study period, for a reflection session together with their team leader. They will ask themselves the following generic questions:

- Did our shift today proceed better than the average of last period? Why?
  - What were the circumstances for the difference?
- Which of the identified circumstances could occur again in the future?
  - What can we learn from that?
  - How can we deal with these circumstances and what can we do differently?

For answering these questions, they can use the Resiliencer-punctuality and analyze the numerical punctuality progress in their area. However, reasoning beyond the numerical data can only be done with help of their personal knowledge and notes made during their shift (figure 3 in the center). We record the discussion and analyze it (figure

3 top right side) as described in the previous section. This will result in an explicit knowledge flow, reasoning, learning and action intentions (figure 3 bottom right side). We will compare these results with the explicit knowledge entered in the reporting system and verified through interviews (figure 3 bottom).

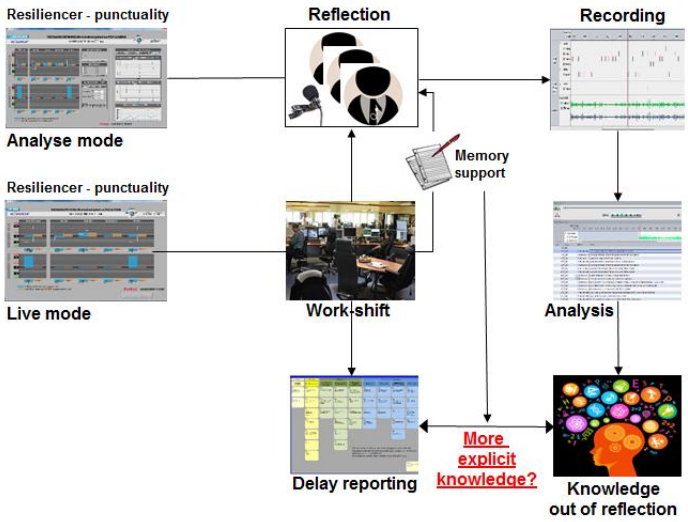


Figure 4 Illustration of study design

4 DISCUSSION

The main challenge of the team reflection analysis is to show that explicit knowledge expressed during the reflection relates to resilience. Resilience is defined, among others, as the behavior of the STS near and beyond its boundaries (Woods, 2006). This leads to the assumption that knowledge arisen through discussion on movements towards and from these boundaries, relates to resilience by definition. However, this theoretical reasoning still needs confirmation. The first approach identifies cases where the system gets out of balance, which is a state related to resilience. In these cases we search for issues, which team reflection identified earlier in a previous case. A successful match proves the effectiveness of team reflection, however it needs coincidence. To enlarge our success rate in finding resilience-related knowledge, we use two more approaches. The first of these is comparing knowledge in the reporting system with explicit knowledge as result of team reflection. We assume that more and deeper reasoning of the latter improves the resilience of the system, since it can be of use when adaptation is needed. The second added approach is based upon Hollnagel's (2009b) cornerstones of learning and anticipation. We will seek for reasoning and induction with the new knowledge, being a component of learning (Felder & Henriques, 1995). Suggestions and opinions approve the intent for anticipation. The combination of these approaches should support the hypothesis that team reflection, on movements towards boundaries, increases resilience of the rail socio-technical system.

Acknowledgements

We greatly appreciate the guidance and review comments by Alfons Schaafsma. This research was conducted within the RAILROAD project and was supported by ProRail and the Netherlands organization for scientific research (NWO) (under grant 438-12-306).

REFERENCES

Bracco, F., Piccinno, T. F., & Dorigatti, G. (2014). Turning variability into emergent safety: The resilience matrix for providing strong responses to weak signals. In 5th Resilience Engineering Symposium (pp. 23–27). Retrieved from http://hdl.handle.net/1811/60454

Chi, M. T. H. (1997). Quantifying qualitative analyses of verbal data: A practical guide. Journal of the Learning Sciences, 6(3), 271–315. doi:10.1207/s15327809jls0603_1

Cowley, S., & Borys, D. (2014). Stretching but not too far : Understanding adaptive behaviour using a model of organisational elasticity. Journal of Health and Safety, Research and Practice, 6(2), 18–22.

Day, R. E. (2005). Clearing up “implicit knowledge”: Implications for knowledge management, information science, psychology, and social epistemology. Journal of the American Society for Information Science and Technology, 56(February), 630–635. doi:10.1002/asi.20153

Dekker, S. (2011). Drift into failure - from hunting broken components to understanding complex systems. Farnham, Surrey: Ashgate Publishing Limited.

Ellis, S., Carette, B., Anseel, F., & Lievens, F. (2014). Systematic reflection: Implications for learning from failures and successes. Current Directions in Psychological Science, 23(1), 67–72. doi:10.1177/0963721413504106

Ericsson, K. A., & Simon, H. A. (1993). Protocol analysis: Verbal reports as data (revised ed.). Cambridge, Massachusetts: MIT Press.

Felder, R. M., & Henriques, E. R. (1995). Learning and Teaching Styles. Foreign Language Annals, 28(1), 21–31.

Frappaolo, C. (2008). Implicit knowledge. Knowledge Management Research & Practice, 6(October 2007), 23–25. doi:10.1057/palgrave.kmrp.8500168

Goverde, R. M. P. (2005). Punctuality of railway operations and timetable stability analysis. PhD thesis. Delft University of Technology. Retrieved from http://repository.tudelft.nl/view/ir/uuid:a40ae4f1-1732-4bf3-bbf5-fdb8dfd635e7/

Hall, J. L. (2003). Columbia and Challenger: organizational failure at NASA. Space Policy, 19(4), 239–247. doi:10.1016/j.spacepol.2003.08.013

Hansen, I. A. (Ed.). (2010). Timetable Planning and Information Quality. WIT Press.

Hollnagel, E. (2008). Safety management - looking back or looking forward. In E. Hollnagel, C. P. Nemeth, & S. Dekker (Eds.), Resilience Engineering Perspectives, Volume 1: Remaining Sensitive to the Possibility of Failure (pp. 63–77). Hampshire: Ashgate Publishing Limited.

Hollnagel, E. (2009a). The ETTO principle: efficiency-thoroughness trade-off: why things that go right sometimes go wrong. Farnham, Surrey: Ashgate Publishing, Ltd.

Hollnagel, E. (2009b). The four cornerstones of resilience engineering. In C. P. Nemeth, E. Hollnagel, & S. Dekker (Eds.), Resilience Engineering Perspectives. Volume 2: Preparation and restoration (pp. 117–134). Farnham, Surrey: Ashgate Publishing Limited.

Polanyi, M. (1969). Knowing and being: In M. Grene (Ed.), Essays by Michael Polanyi (p. 264). Chicago: University of Chicago Press.

Reymen, I. M. M. J. (2003). Research on design reflection: overview and directions. In DS 31: Proceedings of ICED 03, the 14th International Conference on Engineering Design, Stockholm (pp. 1–10).

Schippers, M. C., Den Hartog, D. N., & Koopman, P. L. (2007). Reflexivity in teams: A measure and correlates. Applied Psychology, 56(2), 189–211. doi:10.1111/j.1464-0597.2006.00250.x

Schippers, M. C., Edmondson, A. C., & West, M. A. (2014). Team reflexivity as an antidote to team information-processing failures. Small Group Research, 45(6), 731–769. doi:10.1177/1046496414553473

Siegel, A. W., & Schraagen, J. M. C. (2014a). A method to reveal workload weak-resilience-signals at a rail control post. In D. Harris (Ed.), HCII 2014 (pp. 82–93). Springer Berlin Heidelberg. doi:10.1007/978-3-319-07515-0

Siegel, A. W., & Schraagen, J. M. C. (2014b). Measuring workload weak resilience signals at a rail control post. IIE Transactions on Occupational Ergonomics and Human Factors, 2(3-4), 179–193. doi:10.1080/21577323.2014.958632

Stanton, N. A., & Walker, G. H. (2011). Exploring the psychological factors involved in the Ladbroke Grove rail accident. Accident; Analysis and Prevention, 43(3), 1117–27. doi:10.1016/j.aap.2010.12.020

Weick, K. E., & Sutcliffe, K. M. (2007). Managing the unexpected: Resilient performance in an age of uncertainty, 2nd edition. San Francisco, CA: John Wiley & Sons, Inc.

West, M. (2000). Reflexivity, revolution and innovation in work teams. In M. M. Beyerlein, D. A. Johnson, & S. T. Beyerlein (Eds.), Product development teams (Vol. 5, pp. 1–29). Stanford, CT: JAI Press.

Wiedow, A., & Konradt, U. (2010). Two-dimensional structure of team process improvement: Team reflection and team adaptation. Small Group Research, 42(1), 32–54. doi:10.1177/1046496410377358

Woods, D. D. (2006). Resilience engineering: Redefining the culture of safety and risk management. Human Factors and Ergonomics Society Bulletin, 49(12), 1–8.

CLASSIFICATION AND ASSESSMENT OF SLACK: IMPLICATIONS FOR RESILIENCE

Tarcisio Abreu Saurin[1]
[1] Federal University of Rio Grande do Sul, Av. Osvaldo Aranha 99, 5. andar, CEP 90035-190, Porto Alegre, RS, Brazil
[1] saurin@ufrgs.br; Tel: +55-51-9628-2554

Abstract

Slack is a key concept for resilience engineering (RE), since it can provide resources for dealing with both expected and unexpected variability. However, in complex systems slack interacts with other elements, and this can imply unexpected impacts, which are not necessarily good for safety and efficiency. As such, slack has an ambiguous nature, and a theory of slack using a RE perspective is necessary. This paper has the objective of contributing to the development of the said theory, by introducing a classification and guidelines for the assessment of slack. An example of using the classification in the pharmacy of a hospital illustrates its applicability. Future studies will focus on the investigation of the extent to which the presented framework is conceptually compatible with RE, empirically justified and motivating for action.

1 INTRODUCTION

Complex socio-technical systems (CSSs) are known for tightly-coupled processes, which at the same time account for increased efficiency and facilitate variability propagation in unexpected ways (Perrow, 1984). Tight-coupling usually means the system has little or no slack, which in turn can be a contributing factor to accidents. For instance, NASA´s policy of being "faster, cheaper, and better", ultimately implied slack was gradually degraded, thus introducing brittleness in the system that culminated in the Columbia accident (Woods, 2006). In fact, slack can make systems more loosely-coupled, since it can absorb the impacts of both expected and unexpected variability, providing time and other resources that can support performance adjustment, which is a core characteristic of resilient systems. Furthermore, the need for slack is implicit in the principle of defense-in-depth (Reason, 1997), a well-known safety practice in CSSs. Indeed, by providing multiple barriers and decoupling processes, slack can either slow down the speed of variability propagation or completely block it.

However, slack has its own drawbacks. For instance, it can increase a systems´ opaqueness, disguising small changes and latent hazards which may have non-linear effects (Saurin et al., 2013). Also, badly designed, misused or excessive slack can constitute waste. A number of process improvement methods are focused on the elimination of slack that accounts for waste. From the perspective of these methods, the need for slack is a consequence of unreliable and unstable processes, and therefore the assumption is that slack can be gradually reduced as processes stabilize. Furthermore, excessive slack can be detrimental since the effects of disruptions will not be immediately visible, and thus there will be no pressure to control their underlying causes (Liker, 2004). In other words, excessive slack implies a high threshold for detection of variability.

Regardless of the important and ambiguous implications of slack for CSSs, there is no widely accepted theoretical framework for its investigation from the safety management perspective. The literature seems to be mostly focused on specific forms of slack, such as financial resources and work-in-process in manufacturing plants (Goldstein and Iossifova, 2012), without a broader analysis of the concept and without emphasizing its safety implications and trade-offs. This paper has the objective of contributing to the development of the said theory of slack, by proposition categories of slack as well as guidelines for its assessment in CSSs. It is assumed that understanding how different types of slack can be designed and monitored is relevant for proactive resilience engineering (RE), as it contributes to reducing dependency on opportunistic slack.

2 DEFINITION AND CLASSIFICATION OF SLACK

According to Nohria and Gulati (1996) slack is defined as ''the pool of resources in an organization that is in excess of the minimum necessary to produce a given level of organizational output''. While useful, this definition works better for slack formed by resources that can be easily quantified, such as stocks of materials, money, and equipment. For other resources, such as degrees of freedom of employees in relation to standardized work, and cognitive diversity, the definition of what counts as the ''minimum necessary'' is more elusive. Furthermore, the definition by Nohria and Gulati is restrictive as it implies slack necessarily means the addition of extra resources. A less constraining concept is proposed by Fryer (2004), who suggests that slack means available spare resources, of any sort, which can be called on in times of need. Such spare resources do not necessarily mean extra and idle resources, as they may account for existing and strictly necessary resources that may be relocated and used in different ways as needed. This interpretation is in line with the notion that slack can take different forms depending

on the nature of the underlying resources (Voss et al., 2008), and on the potential for deploying the resources in various ways and at the time that they are needed. Based on a literature review, ten categorizations of slack are proposed, as follows:

(i) Origin: slack may be either designed-in, which usually occurs in tightly-coupled systems, or opportunistic, which usually occurs in loosely-coupled systems, in which slack is often intrinsic to their nature (Perrow, 1984). According to Righi and Saurin (2015), designed slack refers to spare resources whose quantity, place of storage/usage, and nature, are standardized and result from decisions made by groups of individuals and supported by management (organizational level). An example of this type of slack can be stocks of medication with a safety margin that is explicitly sized and visually delimited in stock areas. Opportunistic slack refers to isolated and informal initiatives by staff in times of need – e.g. borrowing a specific piece of equipment from another hospital, and the placement of hospital beds in hallways. This type implies creation of slack via local reorganization (Stephens et al., 2011). Thus, designed slack arises from proactive organizational resilience, while opportunistic slack relies on reactive individual and team resilience, which is often overused (Wears and Vincent, 2013).

(ii) Nature of the resources: in principle, any physical or virtual resource may work as slack in a certain context (e.g. astronomers are looking for an Earth 2.0, which may be a slack to Earth in a distant future), although the resources typically considered are time, people, materials, space, and money. Of course, there might be resources which are more elusive and difficult to be quantified, such as perspectives to solve a problem, and degrees of freedom in standardized operating procedures.

(iii) Availability: slack may be either immediately available or not. Availability is easier if slack is near to the point of use and decentralized, which tends to favor performance adjustment. Another characteristic of available slack is that the resources are not yet committed to organizational design or specific expenditure – e.g. excess liquidity (Cheng and Kesner, 1997).

(iv) Strategy of deployment: five broad strategies were identified. The first strategy, redundancy, may be divided into several sub-categories, such as standby redundancy, active redundancy, and duplication of functions (Clarke, 2005). Clarke provides definitions focused on human redundancy, although the strategy applies to other resources. Standby human redundancy implies the redundant individual is not immediately involved in the task at hand, is typically not present in the operator´s immediate environment, and must be called when necessary (Clarke, 2005) – if the resource in standby is neither loaded nor operational (offline), this strategy may be referred to as ‘‘cold redundancy’’ (Hoepfer et al., 2009). Active redundancy means the individual fulfilling a redundant function is involved in the task at hand – e.g. a worker carries out a task while another monitors the performance of that operator (Clarke, 2005). Hoepfer et al. (2009) refer to active redundancy as ‘‘hot redundancy’’, to convey that the redundant component is fully loaded and operational. Duplication of functions refers to situations in which two different units perform the same function (Clarke, 2005).

The second strategy for the deployment of slack is through the design of work-in-process (WIP), which refers to the creation of queues between workstations. In fact, this strategy is widely used in manufacturing plants, and it usually accounts for stocks of materials in different processing stages – e.g. stocks of raw materials, partially processed products, and finished products. In manufacturing, the size of WIP is normally a function of the stability of processes; the more unstable, the greater the stocks. In workplaces that adopt the lean production philosophy WIP has a standardized limit, and once these limits are achieved, operations must stop functioning in order to avoid overproduction (Liker, 2004).

The third strategy refers to three types of margins of maneuver, suggested by Stephens et al. (2011). Margin of maneuver type 1 is characterized by maintain local margin by restricting other units´ actions or borrowing other units´ margin. Margin type 2 accounts for autonomous strategies to create margin via local reorganization or expand a unit´s ability to regulate its margin. Type 3 refers to coordinated, collective action of recognizing or creating a common-pool resource on which two or more units can draw (Stephens et al., 2011). The fourth strategy is conceptual slack or cognitive diversity, which refers to a divergence in analytical perspectives among members of an organization. The fifth strategy is control slack, which implies individual degrees of freedom in organizational activity, with some range of individual action unconstrained by formal structures of coordination or command. The fourth and fifth strategies were proposed by Schulman (1993).

(v) Tolerance: this refers to the threshold of maximum variability which slack may withstand. A large tolerance means variability is not easily detected, to the extent it does not affect the system´s output. The notion of high tolerance has a parallel with the idea of graceful extensibility, which is characteristic of resilient systems (Woods, 2006). It is also worth noting that tolerance does not necessarily depend on the number of items that form slack (e.g. number of people), but rather it depends on the effectiveness of these items in their role as slack.

(vi) Visibility: the status of existing slack should be easily and quickly visible in the workplace (i.e. at a glance), in order to support performance adjustments triggered by scarcity of resources. A study by Righi and Saurin (2015) found a strong correlation between the need for designing slack and the need for giving visibility to processes and outcomes, in an emergency department. For instance, in this type of environment, staff needs to quickly identify physicians on-duty that can be called in times of need, as well as critical medications that have low stocks. There is a substantial body of knowledge on visual management, which can be useful for the design of visible slack (e.g. Galsworth, 2005).

(vii) Side-effects: in CSSs, elements are highly interconnected and they influence each other. Therefore, the introduction of slack is not a neutral action, making it necessary to assess side-effects, such as new possibilities of error, increased complexity, and maintenance costs arising from slack. In addition to the impact of context, the side-effects of slack may have a relation with the nature of the resources that constitute slack. For example, slack that is formed by physical barriers is prone to have high maintenance costs (Hollnagel, 2004), and it can be brittle under highly dynamic conditions.

(viii) Rate of degradation: while it is not proposed that this category be always quantified, it refers to how long slack maintains its properties even if it is not deployed. A number of factors, which are likely to be dependent on the nature of the resources, can play a role in the rate of degradation. For instance, financial slack may deteriorate due to inflation and unexpected expenditures, slack formed by physical resources (e.g. certain equipment) suffer from wear and tear, and when time means slack, the rate of degradation is expressed in terms of time measurement. Furthermore, it is worth noting that the rate of degradation can be non-linear. This situation may occur, for instance, when unexpected changes in the environment cause an abrupt acceleration/reduction of the pace of consumption of resources (e.g. natural disasters or speculation in financial markets) as well as when technological or organizational changes simply render a given type of slack irrelevant to the intention it was originally devised.

(ix) Breadth: it refers to the breadth of sources of variability that slack can match. The more sources of variability can be matched the more general-purpose the slack is. Again, this category seems to be related to the nature of resources, since some of them are intrinsically more general-purpose – e.g. money can be used to purchase and deploy several types of slack, while fail-safe devices in dangerous equipment are specifically built-in to respond to certain types of human error. An important dimension of breadth is related to the adaptability of slack, which is associated with the idea that slack can self-adjust to dynamic variability.

(x) Hierarchy: in principle, this category seems to be only applicable when there is a linear chain of defenses. In such cases, hierarchy refers to the position of slack along the chain. Slack that forms the first barrier to a certain source of variability is a first-order slack, and so on.

3 GUIDELINES FOR THE ASSESSMENT OF SLACK

In this section, some guidelines for the assessment of slack are presented, as follows:

(a) The values and operational goals of the CSS should be identified. In particular, evidence must be sought of how the efficiency-thoroughness trade-off is usually managed (Hollnagel, 2009), and how the organizational policies state it should be managed. This sets a foundation to determine which types of slack are more important, and which are the acceptable levels of slack. For example, critical equipment on standby might be an asset in an intensive care unit, even if this may be seen as inefficiency from a purely financial viewpoint.

(b) If possible, the assessment should make a distinction between slack-as-imagined (SAI) and slack-as-done (SAD), similarly with the distinction between work-as-imagined as work-as-done, proposed by Hollnagel (2012). The general equation for the assessment of both types is: $\mathbf{SAI\ or\ SAD_{Ri} = Availability_{Ri} - Necessity_{Ri}}$; where R_i = Resource$_i$. This formula recognizes the possibility of negative slack, when the availability is lower than the necessity and the

CSS has to make-do with scarcity of resources. Moreover, the formula makes it clear that negative slack is different from no/zero slack. As an extension of the above formula, the imagined or actual net slack in a CSS may be expressed as: **SAI or SAD Net = ∑ $Slack_{Ri}$**. The value of these formulas is likely to be mostly conceptual, since their operationalization requires the normalization of all types of slack, so as they have a common unit of measurement. Furthermore, due to the dynamics of slack, these calculations should be made for a snapshot of the CSS.

(c) Both the imagined and actual slack should be checked against expected and actual variability, respectively. This may help to identify under and over protected sources of variability.

(d) The assessment should account for the dynamic nature of CSSs. Thus, there should be devised means of capturing how the different types of slack interact and how and why they evolve over time under different conditions. The use of the Functional Resonance Analysis Method (FRAM, by Hollnagel 2012) may be useful for this analysis, as each of the six aspects of the FRAM functions may contain slack – i.e. input, output, control, time, resources, and preconditions. It is also worth noting that changes in slack may be due to the changing goals that are typical of CSSs.

4. AN EXAMPLE OF APPLYING THE CLASSIFICATION OF SLACK

An exploratory study of the central pharmacy of a hospital (Figure 1) illustrates the applicability of the categories for classifying slack. Data collection involved semi-structured interviews with four employees of the pharmacy, about ten hours of direct observations of the functions being carried out, and an analysis of standardized operating procedures (SOPs). The selected example of slack refers to the degrees of freedom of physicians in the function of requesting medications from the pharmacy. While the formal work system design defines specific channels for requesting medications, at predefined times, about 38% of the daily requests (according to data provided by the pharmacy staff) are classified by physicians as urgent. The interviewed employees reported that they do not question the urgency of the prescription, and limit themselves to comply with the physician´s demand. Nevertheless, the employees also reported that they guess, from their experience, whether the urgency is real. Furthermore, the urgent requests made to the pharmacy do not need to be immediately fulfilled, since they do not involve life-threatening situations. In the patient wards there is specific equipment and medications available to deal with acute life threatening situations, such as a cardiac arrest.

Overall, the high incidence of urgent requests for medications seems has consequences, as follows: (i) in line with the SOP, urgent medications may be dispensed and delivered by the pharmacy without the need for checking the prescription for errors; this check is normally made later, only before the second dose of the medication is given, and therefore patient safety is compromised to some extent; (ii) the frequent urgent requests imply staff involved in the dispensation of medications needs to interrupt their workflow, thus being exposed to errors of prospective memory, and delays in the delivery of the regular requests of medications. It also becomes harder for them to follow standardized operating procedures, which would be useful given that the dispensation of medications is a highly repetitive task. Figure 2 presents a summary of the slack classification.

Workstations for checking the medication dispensed – equal stations provide redundancy (duplication of functions) of equipment and employees

Figure 1. Overview of the pharmacy

Classification of slack/Description	Requests of urgent medications from the pharmacy
Origin	The possibility of requesting urgent medications is designed in the system, although it leaves room for opportunistic use, since physicians can decide when and how frequently urgent requests are made
Nature of resources	SOPs, which describe how urgent requests should be made

Classification of slack/Description	Requests of urgent medications from the pharmacy
Availability	Physicians can make an urgent request at any time, and the target set by the hospital is to deliver urgent requests in less than 20 minutes. However, no control is made of how frequently that target is achieved
Strategy of deployment	There is control slack, to the extent that physicians have freedom to make an urgent request at any time. Furthermore, the medications stored in the pharmacy work as a form of standby redundancy, since they are not present in the workplace where they are needed; they are only moved there when necessary
Tolerance	The maximum possible number of urgent requests to be handled by the pharmacy, on a daily basis, is unknown. Currently, about 40% of the daily requests are tagged as urgent
Visibility	Information of how many requests are urgent, and which requests are urgent, can only be accessed through the computerized system – a filter can be applied to show the urgencies. This makes it difficult to evaluate, on real-time, how close the system is to its performance limits. Moreover, there is no visual device to identify, at a glance, which dispensed medication is urgent and which is not; the bags containing the medications look all the same
Side-effects	As previously discussed, the high use of this type of slack creates hazards for patients, reduces the productivity of staff at the pharmacy, and hinders the credibility of urgent requests, which may sometimes not be taken seriously by pharmacists – in fact, there is a parallel between this situation and the incidence of false alarms (i.e. false urgencies, in this case), which occurs in other sectors.
Rate of degradation	The historical evolution of the extent to which this slack is used, was not evaluated. If the percentage of requests classified as urgent has increased over time, this indicates that the consumption of this slack is increasing too. The breaking point of this slack might be an adverse event related to patient safety – e.g. caused by not checking the prescriptions, by delivering an urgent request too late, by delivering and administering wrong medications
Breadth	The possibility of making urgent requests can be useful for dealing with a wide range of sources of variability, such as an unexpected evolution of the patient´s condition, the improper handling of medications and equipment in the hospital´s units, and even delays in the processing of the normal requests within the pharmacy – in this case a normal request may become urgent. However, since physicians do not need to justify the reason for the urgency, there is no available data on the relative incidence of these sources of variability
Hierarchy	The position of this slack in the chain of barriers depends on the reason for the urgent request. For instance, if the medication given to the patient either did not work or was mishandled (e.g. it slipped out of a nurse´s hand and fell on the floor) , the urgent request for a substitute medication from the pharmacy may be a first-level slack

Table.1. Example of applying the categories for classifying slack

6 CONCLUSIONS

This paper presented a classification and guidelines for assessing slack, so as to contribute for developing a theory of slack using a resilience engineering (RE) framework. An example of applying the classification in a hospital pharmacy illustrates its applicability. Future studies will focus on the investigation of the extent to which the framework presented in this paper is conceptually compatible with RE, empirically justified and motivating for action. Also, the FRAM will be jointly used with the proposed framework, in order to support the investigation of how different types of slack could either facilitate or dampen variability propagation.

REFERENCES

Cheng, J. & Kesner, I. (1997). Organizational slack and response to environmental shifts: the impact of resource allocation patterns. *Journal of Management*, 23 (1), 1-18.

Clarke, D. (2005). Human redundancy in complex, hazardous systems: a theoretical framework. *Safety Science*, 43, 655-677.

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.

Galsworth, G. (2005). *Visual Workplace Visual Thinking*. Lean Enterprise Press, Portland.

Goldstein, S. & Iossifova, A. (2012). Ten years after: interference of hospital slack in process performance benefits of quality practices. *Journal of Operations Management*, 30, 44-54.

Hoepfer, V., Saleh, J. & Marais, K. (2009). On the value of redundancy subject to common-cause failures: toward the resolution of an on-going debate. *Reliability Engineering and System Safety*, 94, 1904-1916.

Hollnagel, E. (2012). *FRAM: the Functional Resonance Analysis Method: Modeling complex socio-technical systems*. Burlington, Ashgate.

Hollnagel E. (2009). *The ETTO Principle: efficiency-thoroughness trade-off*. Surrey: Ashgate.

Hollnagel, E. (2004). *Barriers and Accident Prevention*. Aldershot, UK: Ashgate.

Liker, J. (2004). *The Toyota Way: 14 management principles from the world's greatest manufacturer*. New York: McGraw-Hill.

Nohria, N. & Gulati, R. (1996). Is slack good or bad for innovation? *Academy of Management Journal*, 39(5), 1245–1264.

Perrow, C. (1984). *Normal Accidents*: living with high-risk technologies. Princeton University Press, Princeton.

Reason, J. (1997). *Managing the risks of organizational accidents*. Burlington: Ashgate.

Righi, A. & Saurin, T.A. (2015). Complex socio-technical systems: characterization and management guidelines. *Applied Ergonomics*, 50, 19-30.

Saurin, T. A., Rooke, J. & Koskela, L. (2013). A complex systems theory perspective of lean production. *International Journal of Production Research*, 51, 5824-5838.

Schulman, P.R. (1993). The negotiated order of organizational reliability. *Administration and Society*, 5 (3), 353 - 372.

Stephens, R.J., Woods, D.D., Branlat, M. & Wears, R.L. (2011). Colliding dilemmas: interactions of locally adaptive strategies in a hospital setting. *Proceedings of the 4th Symposium of Resilience Engineering*: p 256 -262. Sophia Antipolis, France.

Voss, G. B., Sirdeshmukh, D., & Voss, Z. G. (2008). The effect of slack resources and environmental threat on product exploration and exploitation. *Academy of Management Journal*, 51(1), 147–164.

Wears T. & Vincent, C. (2013). Relying on resilience: too much of a good thing. In: *Resilient Health Care*, Hollnagel E, Braithwaite J, Wears R (Eds.). p. 135-144. Ashgate, Dorchester.

Woods, D. (2006). Essential characteristics of resilience. In: Hollnagel E, Woods D, Leveson N. (Eds.). *Resilience engineering: concepts and precepts*. Aldershot: Ashgate Publishing; 2006. p. 21-34.

A QUANTITATIVE RESILIENCE FRAMEWORK FOR INTERDEPENDENT NETWORKS

D. Hutchison, Lancaster University, U.K.
P. Smith, AIT, Austria
P. Van Mieghem, Delft University of Technology, the Netherlands
R.E. Kooij, Delft University of Technology, the Netherlands
Giorgio Ventre, University of Napoli Federico II, Italy

Abstract

Resilience evidently cuts through several thematic areas, such as information and network security, fault-tolerance, dependability, and network survivability. Significant research efforts have been devoted to these themes, typically by confining to specific mechanisms for resilience and to subsets of the challenge space. We refer to Sterbenz et al [1] for a discussion on the relation of various resilience disciplines, and to a survey on network resilience by Cholda et al [2]. A shortcoming of existing research and deployed systems is the lack of a systematic view on resilience, to engineer networks that are resilient to challenges that transcend those considered by a single thematic area. A non-systematic resilience approach that does not cover thematic areas, leads to an impoverished view on resilience objectives, potentially resulting in ill-suited solutions. Additionally, a patchwork of resilience mechanisms, incoherently devised and deployed, can result in undesirable behaviour and an increased management complexity, encumbering the overall network management task [3]. Smith et al [4] argue for resilience as a critical and integral property of networks. They adopted a systematic approach to resilience, which takes into account the wide-variety of challenges that may occur. The core of this approach consists of a coherent resilience framework, which includes implementation guidelines, processes, and toolsets to underpin the design of resilience mechanisms at various levels in the network. Central to the framework is a control loop, which defines necessary conceptual components to ensure network resilience. The other elements – a risk assessment process, metrics definitions, policy-based network management, and information sensing mechanisms – emerge from the control loop as necessary elements to realise this systematic approach.

Although the framework from [4] is very useful to deal with resilience engineering of networks operating in isolation, in the last few years an increasing awareness penetrates the research community that the critical infrastructures of a nation are closely coupled: the proper functioning of one infrastructure depends heavily on the proper functioning of another [5]. A case in point is the interdependency between the electric power grid and the communication network. The aim of our paper is to sketch how the resilience framework proposed in [4] can be extended to interdependent networks. Besides robustness envelopes [8] and coupling strengths between interdependent networks, an important part of this extended framework will be to incorporate a generic resilience metric, referred to as the R-value in [6], which is a linear combination of several graph metrics that quantify resilience in networks, such as average shortest path length, diameter and assortativity, but also more advanced metrics such as algebraic connectivity or spectral radius. Recently, the R-value concept has been extended, see [7], in order to solve two open issues, namely how to dimension several metrics to allow their summation and how to weight each of the metrics.

The (enhanced) R-value will be used to define a number of resilience classes. A resilience class specifies, for a certain service, a subinterval of [0, 1] since $R \in [0, 1]$. For example, class C1 contains all graphs whose R-values lie between [0, r1], class C2 contains all graphs in [r1, r2], and so on. The rationale behind resilience classes is that a small number of classes is more manageable than a continuous range of R, and they ease interpretations by mapping the R-values to a few ranges such as red, orange, green with their usual meaning.

REFERENCES

[1] J.P.G. Sterbenz, D. Hutchison, E.K. Çetinkaya, Abdul Jabbar. J.P. Rohrer. M. Schöller, P. Smith, “Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines,” Elsevier Computer Networks, Special Issue on Resilient and Survivable Networks, vol. 54, no. 8, June 2010, pp. 1243–42.

[2] P. Cholda, A. Mykkeltveit, B.E. Helvik, O. Wittner, “A Survey of Resilience Differentiation Frameworks in Communication Networks,” IEEE Communications Surveys & Tutorials, vol. 9, no. 4, 2007, pp. 32–55.

[3] ENISA Virtual Working Group on Network Providers’ Resilience Measures, “Network Resilience and Security: Challenges and Measures,” tech. rep. v1.0, Dec. 2009.

[4] P. Smith, D. Hutchison, J.P.G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, B. Plattner, “Network Resilience: A Systematic Approach”, Communications Magazine, IEEE, Volume 49, Issue 7, pp. 88-97, July 2011.

[5] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, S. Havlin, “Catastrophic cascade of failures in interdependent networks,” Nature, vol. 464, no. 7291, pp. 1025–1028, 2010.

[6] P. Van Mieghem, C. Doerr, H. Wang, J. Martin Hernandez, D. Hutchison, M. Karaliopoulos,

R. E. Kooij, “A Framework for Computing Topological Network Robustness”, Delft University of Technology, report 20101218, 2010.

[7] M. Manzano, F. Sahneh, C. Scoglio, E. Calle, J. L. Marzo, “Robustness surfaces of complex

networks”, Nature Scientific Reports, Volume, 4, Article number: 6133, doi:10.1038/srep06133, 2014.

[8] S. Trajanovski, J. Martin-Hernandez, W. Winterbach and P. Van Mieghem, “Robustness Envelopes of Networks”, Journal of Complex Networks, Vol. 1, pp. 44-62, 2013.

SOCIO-TECHNICAL SYSTEM RESILIENCE ASSESSMENT AND IMPROVEMENT METHOD

Eric RIGAUD [1], Christian Neveu[2], Stella Duvenci Langa[2], Marie Noelle Obrist[2 1] MINES ParisTech, PSL Research University, CRC, Centre de
recherche sur les risques et les crises, CS 10207 rue Claude Daunesse
06904 Sophia Antipolis Cedex, France
[1] eric.rigaud@mines-paristech.fr / +334 93 95 74 86
[2] SNCF – Direction Sécurité Système et Projets Département Management Facteurs Humains et Europe 20 rue de Rome 75008 PARIS

Abstract

Resilience is an integrative concept that appeared in 21st century scientific thinking and encompasses two main ideas: response to stressful events and sustainability of systems in coping with stressful events (Reich et al., 2010). There is no consensus on a common definition of system resilience. Resilience is sometimes considered as a process, as a characteristic of system, as a dynamic of development, as an outcome and sometimes all of the above (Zautra et al. 2010). To be resilient, a system has to be exposed to significant threats or severe adversity and achieve a successful adaptation despite negative conditions (Luthar et al. 2000). Resilience related definitions, models and artifacts vary according to the diversity and the complexity of systems (technological devices, individuals, groups, work situations, organizations, communities, states, territories, etc.), of threats (natural, technological, entropic, economical, anticipated, surprise, etc.) and of adaptation modes (routines, compliance to rules, improvisation, return to a stable state, transformation, etc.).

Theories of Resilience has been developed with perspectives of improving safety performance and safety management systems in management sciences (Wildavsky 1988, Weick 1998, Weick et Sutcliffe 2007), in safety sciences (Hollnagel et all 2006, 2011) and in disaster and crisis management sciences (Confort et all. 2010). Some works on the definition of resilience are related to specific capacities: “capacity to cope with unanticipated dangers” (Wildavsky 1988), “capacity to improvise”, to “bounce back” (Weick 1998), “monitoring the boundary conditions of the current model for competence and adjusting or expanding that model to better accommodate changing demands” (Woods 2006), whereas other works aim to integrate all capacities required to be safe: “the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions” (Hollnagel et all. 2011).

The aim of the proposed paper is to describe a framework for assessing and improving socio-technical system resilience. The framework is the result of an ongoing process aiming to develop methods and tools based on Resilience Engineering concepts and models. Framework presented is the result of the refinement of an initial method based on the Resilience Analysis Grid (Hollnagel 2011) and presenting some limitations identified after an initial experimentation.

The paper will be structured in three parts.

The first part is dedicated to the presentation of the theoretical background used for developing the method. The four initial cornerstone of system resilience has been refined in order to characterize nine dimensions: system capacity to respond to the variability of its environment, system capacity to respond to unwanted event, system capacity to monitor performance of the past, system capacity to monitor actual performance, system capacity to monitor potential performance, system capacity to learn from unwanted situation from the past, system capacity to learn from daily situation, system capacity to prevent impact of change on resilience performance, system capacity to prevent impact of evolution on resilience performance.

The second part is related to the presentation of the nine indicators of the method. Each indicators is structured with five levels allowing the definition of an assessment process. Each level corresponds to a set of concrete properties that will structure the evaluation of the resilience property of a system.

The third and final part presents the methodological guideline aiming to structure data collection processes and analysis allowing producing a profile and a plan of actions for improving the resilience of a system. Four phases are described: Definition of the context of the study, data collection, system diagnostic and actions plan design.

REFERENCES

Boin A., Comfort L. K., Demchak C., 2010. The rise of resilience, in Comfort L.K., Boin A., Demchak C.C., (eds.), Designing resilience, preparing for extreme events, University of Pittsburgh Press.

Hollnagel E., 2011. Prologue: The Scope of Resilience Engineering, in Hollnagel E., Pariès J., Woods D. D. and Wreathall J., Resilience Engineering in Practice. Ashgate Studies in Resilience Engineering.

Weick, K. E. and Sutcliffe, K. M. 2001. Managing the unex- pected: assuring high performance in an age of complexity. San Francisco.

Woods D. D., 2006. Essential Characteristics of Resilience, in Hollnagel E., Woods D., Leveson N., Resilience Engineering: Concepts and Precepts, Ashgate.

TRAINING, EDUCATION, SIMULATION, SERIOUS GAMES

DEVELOPING RESILIENCE SKILLS THROUGH SCENARIO-BASED TRAINING: A COMPARISON BETWEEN PHYSICAL AND VIRTUAL SCENARIOS

Priscila Wachs[1], Angela Weber Righi[2], Tarcísio Abreu Saurin[3], Eder Henriqson[4], André Manzolli[5], Felipe Taborda Ribas Tovar[6], Fabio Yukio Nara[7], Eduardo Massashi Yamao[8], Luis Gustavo Tomal Ribas[9] and Harlen Feijó Bório[10]
[1, 2, 3] Federal University of Rio Grande do Sul, Av. Osvaldo Aranha 99, 5. andar, CEP 90035-190, Porto Alegre, RS, Brazil
[1]priscilawachs@ig.com.br, [2]angelawrighi@yahoo.com.br, [3]saurin@ufrgs.br
[4]PUCRS (Pontifical Catholic University of Rio Grande do Sul), Av. Ipiranga, 6681, CEP 90619-900 Porto Alegre, RS, Brazil
[4]ehenriqson@pucrs.br
[5,6,7,8,9,10]Institutos Lactec (Mechanical Systems Division (DVSM), Mechanics Department (DPME), Rodovia BR 116, km 98, nº 8813, CEP 81530-180, Curitiba, PR.
[5]manzolli@lactec.org.br, [6]felipe.ribas@lactec.org.br, [7]fabio.nara@lactec.org.br, [8]eduardo.yamao@lactec.org.br, [9]luis.gustavo@lactec.org.br, [10]hfborio@lactec.org.br

Abstract.
The aim of this study is to present a new application of a method for developing resilience skills (RS) through scenario-based training (SBT). This application used virtual scenarios for training hydroelectric power plant operators. Based on this, it was possible to compare the results with an earlier application of the same method for training grid electricians, using physical scenarios. The SBT method adopted in both contexts consisted of: (i) identifying RS, work constraints, and actions for redesigning the socio-technical system; (ii) developing template scenarios; (iii) developing protocols for undertaking the simulation and assessing trainees´ performance; and (iv) testing and refining the scenarios and the protocol. The different simulation technologies are compared, stressing implications for the training of RS.

1 INTRODUCTION

Contemporary sociotechnical systems (STS) are characterized by their complexity, resulting from factors such as the growing scale of operations, intense use of information technology and a changing external environment (ElMaraghy et al., 2012; Carayon, 2006). Under these conditions, resilience is essential in order to compensate for the difficulties created by complexity. Although complex sociotechnical systems (CSS) are resilient by nature, conditions that favour resilience can be created by applying suitable managerial and technological practices.

This article addresses training in resilience skills (RS), a practice that can support individual, team and organizational resilience. Scenario-based training (SBT), in turn, is a means of developing RS since it enables the simulation of realistic scenarios, providing systematic and structured learning experiences as well as an appropriate measurement and feedback system (Zendejas et al., 2010; Salas et al., 2008).

As such, the objectives of this study are twofold: to present a new application of a SBT method for RS development proposed by Saurin et al. (2014); and to compare two types of technologies for SBT, one using physical scenarios and the other applying virtual ones. This discussion is based on case studies of the electricity sector.

2 CONTEXT OF THIS STUDY

Training using physical scenarios was conducted in an electricity distribution company, focusing on the work of grid electricians carrying out emergency maintenance on the grids. Virtual training was carried out in an electricity generation company, focusing on the work of hydroelectric power plant operators.

The SBT method adopted in both projects consisted of the following stages: (i) identifying RS, work constraints, and actions for redesigning the STS (ii) developing template scenarios; (iii) developing protocols for undertaking the simulation and assessing trainees´ performance; and (iv) testing and refining the scenarios and the protocol. This method is described in the study by Saurin et al. (2014), which reports the application of SBT in the aforementioned power distribution company using physical scenarios. The present study also consists of a new application of that method, in a hydroelectric power plant using virtual scenarios.

3 Overview of the work carried out by grid electricians and hydroelectric power plant operators

Concerning *the electricians from the emergency maintenance teams,* demand for services of these teams usually starts with phone calls from customers to the Customer Service Call Center, which sends a service order, via a computerized system, to the operations center. Then, the central operations control room analyses the information and contacts the team that are nearest the place where the call came from.

The teams are formed by a pair of electricians, who await a call from the central operations in vehicles in different areas of the city. Typically, a customer's request is about power shortage and, sometimes, due to damages to the infrastructure of the distribution network, such as rupture on the power line.

Concerning the hydroelectric power plant operators, two operators per shift control the dam from a control room within the dam structure itself. One operator served as the command room controller and remained in the plant's control room for his entire shift, primarily responsible for the supervisory controllers that operate the power generating turbines. The machine room operator is responsible for inspecting plant sites and measuring equipment performance, as well as manually operating machinery when necessary. Thus, while the control room operator stays in the control room the whole shift, the machine room operator leaves the room periodically to inspect the power plant or manually operate equipment.

The hydroelectric power plant used as a reference in this study for the development of the simulation has three Kaplan turbines generating a total of 136.8 MW. The dam is 856.25m long and the reservoir covers 63 km² (considered a run-of-the-river plant), with seven surface and three underwater floodgates.

4 training program development

4.1 Resilience skills, work constraints and actions for redesigning the socio-technical system

Cognitive Task Analysis (CTA) was used to identify RS, work constraints, and actions for redesigning the STS (stage i), involving interviews (Critical Decision Method), observations of actual work and document analysis (table 1). Wachs et al. (2012) present details on the process of data collection and analysis for stage (i).

Table 1. Data sources

	Power distribution company	Hydroelectric power plant
Interviews	13 interviews with electricians (done with pairs of electricians, total of 24 different participants) ≈20 hours of audio	8 interviews with operators ≈9 hours of audio
Observations	20 hours of field work 30 hours of training course	40 hours of field work (control room and machine room)
Document analysis	work instructions, standard operating procedures, safety procedures, job-related responsibilities, incident reports	work instructions, standard operating procedures, safety procedures, job-related responsibilities

In the case of grid electricians, 12 RS categories (with 105 examples, which account for practical examples of RSs, so workers could find them meaningful and easy to understand), 14 constraint categories and 15 actions for redesigning the socio-technical system were identified. As for hydroelectric plant operators, 11 RS categories (69 examples), 6 categories of constraints and 7 actions for redesigning the socio-technical system were identified (appendix 1).

Although the study in the hydroelectric power plant identified fewer RS and constraints, this does not necessarily mean it is less complex than the electricity distribution context. On the one hand, the work carried out in these plants takes place in a more controlled environment with less direct influence from factors such as population and difficult access. On the other hand, activities at hydroelectric power plants involve a significant number of dynamically interacting control parameters, such as voltage, flow, floodgates, river levels, and climate influences. For example, 795 command operations were incorporated in the computer platform for the training scenarios.

Regardless of differences in the number of RS in both contexts, there is a similarity in their nature, such as for RSs related to work strategy: "draw up work strategies to re-establish power plant operations" (hydroelectric

operators) and "draw up work strategies after defects have been identified" (electricians). In both cases variability is inevitable and therefore the need for dealing with events that are not fully covered by standard operating procedures is part of the routine.

4.2 Template scenarios

In stage (ii), template training scenarios were devised with the support of electricians and hydroelectric power plant operators. Template scenarios present the core characteristics required to meet training objectives. Thus, work constraints can be added to template scenarios in order to increase the level of complexity of training sessions (Martin et al., 2011). 3 template scenarios were devised and implemented for the electricity distribution company (physical SBT) and 4 template scenarios for the hydroelectric (virtual SBT). Table 2 presents one scenario for each context and describes its main elements.

For the physical SBT, a network was built, with eight poles, one transformer, and five meters, each simulating one residential client. A tension of 127 V energized the grid and kept bulbs lit up in each client. In order to work in those scenarios, trainees received a vehicle equipped with materials, tools and safety gear.

The computer platform for virtual SBT was developed based on photographs, videos, and sounds (e.g. alarms, vibration of turbines) from a real hydroelectric plant and it accurately depicted the power plant setting. In addition to this, a logical mathematical model was designed to operate the plant, similar to the power plant's actual operating model with 795 commands.

Table 2. Main elements of SBT

	Physical Scenario	Virtual Scenario
Initial Condition	Technical information: Oscillating light in boxes 30 and 50, crossbar 4 or light oscillating in box 50. Consumer information: fridge "does not start", electric shower "does not heat up".	Technical information: ancillary service in generator unit (GU) 3; machines in the system: GU1 (bar I with 40MG), GU2 (bar I with 40MG), GU3 (connected to bar II at 40MG); General Information: time of day: 3 p.m.; climate: fine weather;
Defects/ Problem	Distribution point connector incorrectly sized, defect in the neutral cross connector.	GU3: temperature of 70°, heat exchanger and oil circulation pump in the bearings
Proposed Solution	Change the connectors	Stopped for urgent / emergency work "Request" machine so that stoppage is for urgent (and not emergency) work.
Resources Materials	For the scenario: low voltage grid with five consuming units and s transformer (fig. 1) For learners: equipped truck	Computer platform (software/hardware: LabVIEW, Java and PostgreSQL) (fig. 2), rooms and radios.
Human Resources	Actors: DOC (Distribution Operation Center) and consumer; Trainees: 2 electricians	Actors: Operator from the Operation Control Center (COGE), supervisor (coordinator) and maintenance Trainees: 1 machine room operator and 1 command room operator.

4.3 Protocols for undertaking the simulation and assessing trainees´ performance

Simulation and assessment protocols (stage iii) aimed to: guide the instructor in conducting the simulations, record simulation data and assess the simulation itself and the trainee performance. The simulation involves the following

steps: (a) briefing: opening the simulation session by explaining the training objectives and presenting a general overview of the simulation process; (b) the simulation itself, either physical (figure 1) or virtual (figure 2); and (c) debriefing: once the simulation is completed, the instructor and trainees discuss their performance and learning opportunities, followed by a self-assessment whereby trainees assign scores on a questionnaire and instructor's evaluate the participants based on the same questionnaire.

The debriefing plays a key role from the resilience engineering perspective since it allows the identification of new examples of RS, new work constraints and new actions to re-design the system. In fact, the debriefing is an opportunity to discuss the performance of the joint cognitive system, going beyond the trainees´ individual performance.

The protocols for undertaking the simulation and assessing trainees´ performance present similar steps in both investigated contexts. However, the physical SBT protocols are paper based while the virtual SBT one´s are done through the computer platform. The computer platform permits an automatic record of simulation data, including a timeline containing each operator's commands, providing easy information recovery and filtering, making debriefing easier. Also, it permits the operator´s self-assessment in the platform, speeding up result analysis and comparison.

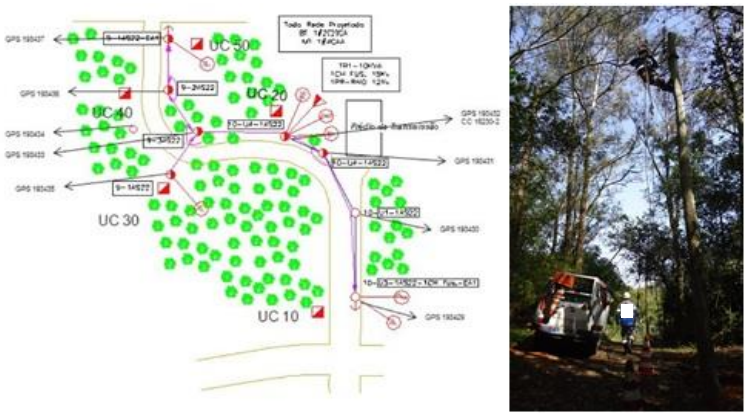


Figure 1. On the left: map given to electricians in the briefing stage of SBT. On the right: view of the electricians during a simulation session

Figure 2 On the left: control room virtual environment. On the right: example of a supervisory screen

4.4 Testing and refining the scenarios and the protocol

The testing phase of physical SBT was completed and the company has used the proposed method as part of their electricians´ formal training. On the other hand, the project involving virtual SBT is in the final stages, still undergoing testing. A total of 18 test simulations were conducted for the physical SBT, while only 3 were done in virtual SBT. In fact, the project related to the hydroelectric power plant was much more time-consuming in terms of data collection and development of the "simulator" (i.e. the computer platform, in this case). Therefore, there was relatively less time available for testing the simulator in practice.

5 Comparison between the two contexts

Developing and conducting SBT using different types of scenarios (physical or virtual) allows the strengths and weaknesses of each technology to be assessed, as shown in table 3.

Table 3. Comparison between the different simulation technologies

Criteria	Physical Scenario	Virtual Scenario
Space	substantial need for physical space, since a full scale network was built	reduced need for physical space, involving just a room for locating the computers and servers (Figure 3)
Physical resources for setting up the simulation	low voltage grid with five consuming units and transformer and equipped truck	simulation room with the computers and communication radios
Time for building the scenarios	less time-consuming for building the network (low voltage grid) – one year	more time-consuming for developing the computer platform three year
Realism of the scenarios	more realistic environmental conditions (e.g. vegetation, lighting, ...)	use of media from the actual environment to ensure greater realism and use of technology to simulate environmental conditions (e.g. night, rain) However, the use of media restricts some realism since a photograph is a static image
Control over work constraints introduced in the simulation	less control over work constraints, although this can be beneficial for RS training, since unexpected scenarios can be created involuntarily	greater control over work constraints
Record of simulation data	manual record of data gathered by the instructor	automatic record of simulation data, including a timeline containing each operator's orders, providing easy information recovery and filtering, making debriefing easier
Assessment	on paper, requiring manual result analysis and comparison	in the platform, speeding up result analysis and comparison

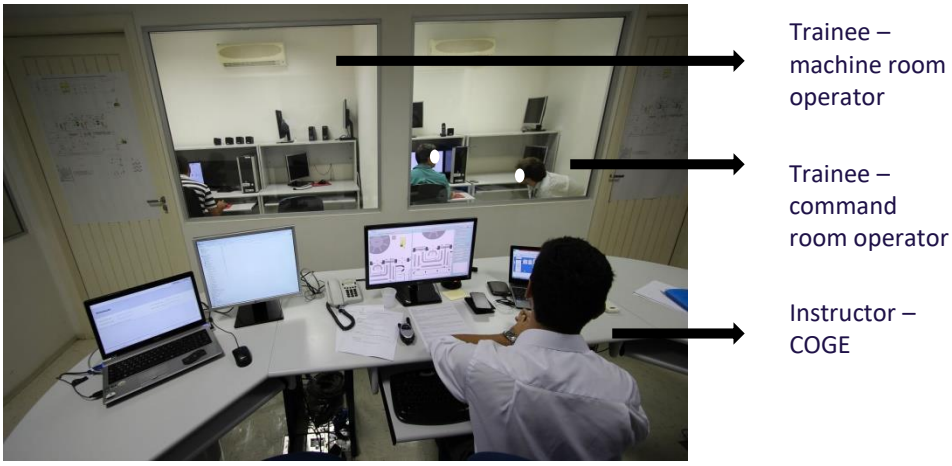


Figure 3. View of the virtual simulation room and participants

6 Conclusions

The focus of this study was to present a new application of a SBT method for RS training and compare two types of technologies for SBT, one using physical simulations and the other applying virtual ones.

The strengths and weaknesses of the simulation technologies may be more related to the context in which each was applied, rather than to the technologies themselves. For example, in the hydroelectric power plant, physical simulation is difficult due to economic and environmental reasons, making simulation using a computer platform a viable alternative. In this case, where the plant is controlled remotely via a computerized operating system, simulation using a computer platform is very similar to the actual work environment.

The results also indicated that the adopted method for SBT is in line with the four basic abilities of resilient organizations described by Hollnagel et al. (2011): responding, monitoring, anticipating and learning. Indeed, the RSs identified in both contexts may be associated with those four abilities. In particular, the ability to learn is developed in the debriefing phase. As such, regardless of the context and simulation technology, this ability can be practiced in the debriefing.

Another important point is to reflect on system redesign suggestions, which can provide organizational support for worker resilience. None of the companies involved in this research committed to or showed interest in applying the phase involving system redesign. This is an important gap from a resilience engineering standpoint, which may indicate how unprepared companies are for this philosophy, focusing on individuals as opposed to the system as a joint cognitive system.

Acknowledgments

We are especially grateful to the electricians, electricians´ training instructors and two directors of the health and safety at work department from the power distributions company, the hydroelectric power plant operators and managers. They provided essential technical inputs for designing the SBT program.

REFERENCES

Carayon, P. (2006). Human factors of complex sociotechnical systems, *Applied Ergonomics*, 37, 4, 525–535.

ElMaraghy, W., ElMaraghy, H., Tomiyama, E. e Monostori, L. (2012), “Complexity in engineering design and manufacturing”, CIRP Annals - Manufacturing Technology, Vol. 61 No. 2, pp. 793–814.

Hollnagel, E.; Paries, J.; Woods, D.; Wreathall, J., 2011. *Resilience Engineering in Practice:* a guidebook. Burlington: Ashgate.

Martin, G. A. & Schatz, S. & Hughes, C. & Nicholson, D. (2011) What is a scenario? Operationalizing Training Scenarios for Automatic Generation. In: Kaber, D.; Boy, G. (Ed.), *Advances in Cognitive Ergonomics* (pp.746-753). London: CRC Press.

Salas, E. & Rosen, M. & Held, J. & Weissmuller, J. (2008). Performance Measurement in Simulation-Based Training: a review of best practices. *Simulation & Gaming*, 40, 3, 328-376.

Saurin, T. & Wachs, P. & Righi, A.W . & Henriqson, E. (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., Righi, A., Saurin, T.A., 2012. Identification of non-technical skills from the resilience engineering perspective: a case study of an electricity distributor. Work, 41, 3069–3076.

Zendejas, B. & Cook, D. & Farley, D. (2010). Teaching First or Teaching Last: Does the Timing Matter in Simulation-Based Surgical Scenarios? Journal of Surgical Education, 67, 6, 432-438.

OBSERVING RESILIENCE: AIR TRAFFIC CONTROL CENTRE CONTRIBUTION TO EVERYDAY OPERATIONS

Martina Ragosta [1]
[1] DeepBlue Srl, Piazza Buenos Aires 20, 00198 Roma - Italy
[1] martina.ragosta@dblue.it - **+39 320 90 44 747**
http://www.dblue.it/

Abstract

The paper proposes a concrete approach for observing resilience in practice translating the theoretical achievements (e.g. resilience themes and principles) into practical supporting material (i.e. a resilience observation sheet). This material is integrated in a high level experiment protocol for observing resilience through direct observations. In this perspective, resilience is an embedded feature of the system under analysis that should be taken into account in observing humans while they perform daily activities. If resilience belongs to the system, it is a part of it and evolves over time according to several elements and their combination. A deeper understanding and analysis of how humans can manage and adapt in a flexible manner to continue everyday operations is needed. Therefore, it is necessary to identify some practical indicators which can be used as early warnings to diagnose the system status and act timely in order to anticipate and prevent negative outcomes. Accordingly, the suggested protocol is exemplified through its practical application in an operational Air Traffic Control Centre (ATC) everyday activity, the missed approach procedure.

1 INTRODUCTION

As recognised by Theory Z (Hollnagel, 2008), Resilience Engineering (RE) aims at maintaining or improving safety looking at what goes right, as well as on what should have gone right. Theories, models, and methods aim to describe how things go right, but sometimes fail, and how humans and organisations cope with internal and external intractability and unpredictability. In this perspective, Socio-Technical Systems (i.e. an Air Traffic Control Centre which belongs to this class as it encompasses complex interactions involving humans and machines deeply influenced by environmental/organisational aspects) are considered safe and efficient. But a contributing factor to this is that humans learn to overcome the inevitable shortcomings, can adjust their performance to meet the actual demands of a situation, can interpret procedures and apply them to suit actual conditions, can detect when something fails or goes wrong, and can in many cases correct for it as well.

Consequently, humans play a preeminent role which requires further investigation in order to enable users to perform their everyday activities efficiently and effectively. However, due to the complex nature of a STS, task performance may be affected by an inborn variability. This is both normal and necessary and is the source of positive and negative outcomes – successes and failures – alike.

While some adverse events can be attributed to component malfunctions, others arise from unexpected combinations and/or non-linear interactions among normal performance variability of everyday activities. In order to prevent negative outcomes, an identification of the situations where normal performance variability may combine to create unwanted effects and to monitor continuously the status of the STS is needed.

Observing the users in everyday activities can support in identifying some indicators for detecting unwanted effects timely and in using these indicators as early warnings for monitoring the status of the system proactively.

This paper proposes an approach for accomplishing direct observations in an ATC centre during everyday operations. These observations can support in envisioning and detecting some resilience indicators related to performance variability of everyday activities (i.e. a missed approach performed through a go-around manoeuvre). These can be used for understanding the status of the system and to act timely. Due to the fact that an ATC centre can be considered a Socio-Technical System, these indicators cannot be isolated. But for the complex nature of the system under study, resilience indicators are interconnected. For this reason and for better understanding their role and interconnections, they are organised in patterns. Hence, a resilience pattern is a collection of resilience indicators. The patterns are constructed on the basis of current Resilience Engineering concepts as well as findings from the case studies investigated in the SCALES project (Herrera et al., 2014).

This paper outlines the suggested approach, its application through direct observations in an ATC and discusses preliminary findings regarding resilience in practice in terms of indicators and patterns. It starts with a short description of the protocol for observing resilience. Then, it introduces an everyday activity performed by Air Traffic Controllers (ATCOs), namely the missed approach procedure performed through a go-around manoeuvre. After, the protocol is further explained and applied to this case. Finally, results from this application are presented and

discussed. The discussion reflects on added knowledge to identify resilience in practice and in daily activities, theoretical and practical implications.

2 OBSERVING RESILIENCE: A PROTOCOL

The ethnographic approach (Blomberg & Burrell, 2009) emphasises the understanding of behaviour in context through the participation of the investigator in the situation being studied as an observer of the team of users involved in the situation. Direct observation is a non-intrusive technique which allows participants to do what they normally do without being disturbed by the observer that is a "silent" actor "in situ".

This qualitative research answers questions about the complex nature of phenomena, with the purpose of describing and understanding the phenomena from the participants' point of view. Accordingly, multiple methods of data collection may be employed: video- and audio-recording, interviews, and surveys.

During direct observation, commonly the observer is sitting passively and recording as accurately as possible what is going on such as the behaviour of one or more persons, their interactions and the ones with different kind of artefacts. The observation is often supported by grids and guidelines to identify and capture relevant aspects/issues to be recorded.

Once having completed the observation, the observer provides a report, utilising a range of approaches, mainly informal interviews/debriefings and qualitative and quantitative analyses of the gathered information.

In order to properly conduct direct observations, this paper suggests a high-level experiment protocol consisting of several steps. It can be adapted according to objectives and observers' needs as well as supporting materials.

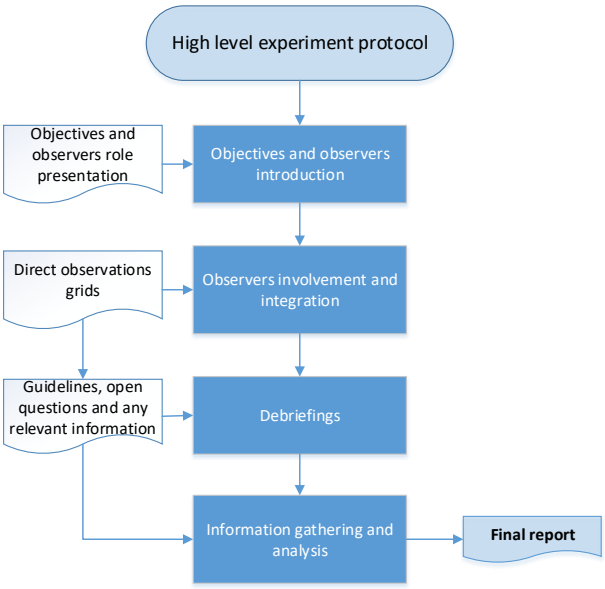


Figure 1. High-level experiment protocol steps, supporting materials and output

3 OBSERVING RESILIENCE IN PRACTICE: THE PROTOCOL APPLICATION

This protocol is exemplified through its practical application in an operational ATC everyday activity, the missed approach. It is a procedure followed by a pilot when an instrument approach cannot be completed to a full-stop landing (FAA, 2013). This must be flown in accordance with the published procedure stated for each runway or following the Air Traffic Control Operator (ATCO) instructions prior to the clearance for the approach. However, if the pilot believes that a missed approach may occur, s/he can make a specific request to ATCO including heading and altitude instructions to avoid in-flight delays and efficiently manoeuvre the aircraft into position for either its next approach, or a diversion to an alternate airport. Missed approach is a common operation but it involves many elements that should be taken into account and managed simultaneously (Herrera et al., 2014a). For this reason, its development and outcome can be unexpected.

Through an extensive literature review and workshops with operational staff, several ATC elements which can contribute to the outcome of the operation have been identified and organised as follows[8]:

[8] Due to space constraints the four main categories and correspondent ATC elements are just briefly summarised.

1. "COMmunication between pilots and ATCOs" (COM) consisting of:
    a. updating relevant information,
    b. the timing of issuing instructions,
    c. the language used.
2. "Management and Control of aircraft" (MC) which includes:
    a. separation and spacing,
    b. stabilised approaches,
    c. vectoring, etc.
3. "Design of Procedures and airspace" (DP) which consists of
    a. the degree of complexity,
    b. potential traps, etc.
4. "Awareness" (A) which includes
    a. information analyses,
    b. sharing information, etc.

These can be used as clues for guiding the observer while is performing her/his task and in filling the "Observation sheet"[9] (Fig.2). Indeed, they are reported in the sheet as "Topics of Interest". In the excerpt (on the right of the Fig.2), an example of the "Observation sheet" filled in.

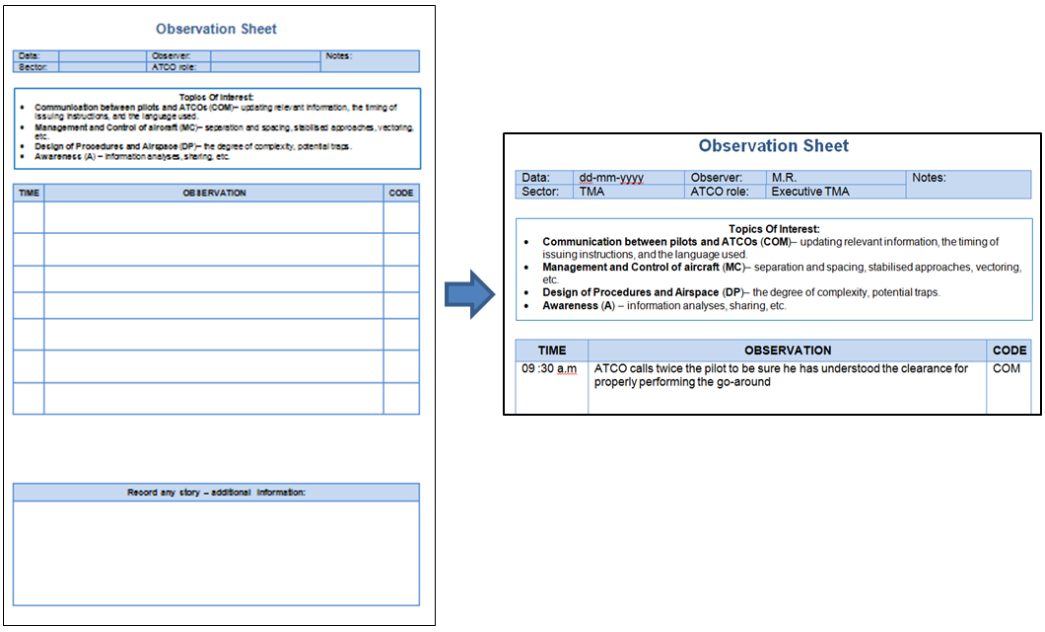


Figure 2. On the left – "Observation sheet" for collecting information during direct observations – On the right, an excerpt of the "Observation sheet" filled in.

This sheet is the supporting material for the second step of the protocol. It helps in capture everyday operations, adaptations, ATC contributing elements, in documenting actions performed by controllers exploring individual, technical and organizational context and stories to illustrate how ATC services are delivered in practice.

Stories are important as a way to expand technical understanding of the behaviour of the ATC e.g. about how unusual things have happened and how the ATC deals with these (adapted from Hayes, 2013).

Once the observation session is ended, the observer can use the "Observation Sheet – Resilience themes & principles mapped to everyday operations" (Fig. 3) as guideline for setting up and leading the conversation during the debriefing in order to further explore the relevant insights with the controllers involved in the operations.

Thanks to the controllers and the observer collaboration, information can be structured and analysed in the RE perspective. Indeed, the sheet offers a preliminary resilience overview consisting of the four main capabilities, that are "Monitor", "Anticipate", "Respond", and "Learn", and boxes where some resilience patterns are further detailed into resilience indicators (Herrera et al. incoming).

[9] Please note that this observation sheet is made for personnel involved in the SCALES project mapping ATC contributions to everyday operations

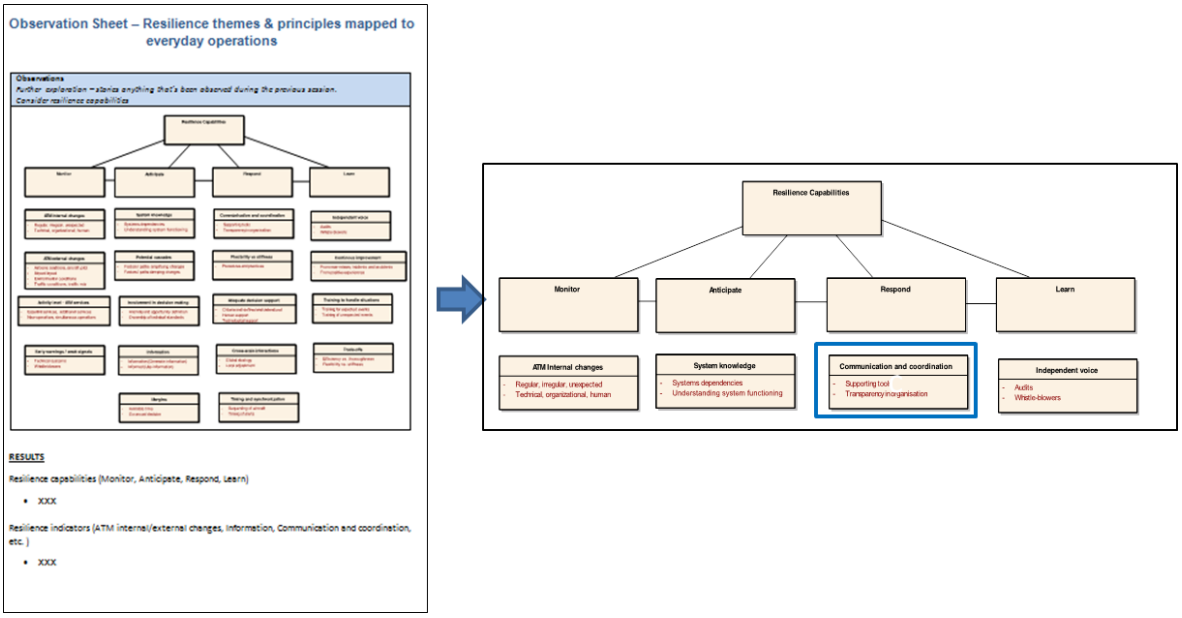


Figure 3. On the left, "Observation Sheet – Resilience themes & principles mapped to everyday operations" for debriefing sessions – On the right, an excerpt of the sheet filled in.

Through this sheet, the recorded ATC contributing elements can be translated into some resilience patterns/indicators. Indeed, the ATC contributing element identified during the observation, "ATCO calls twice the pilot to be sure he has understood the clearance for properly performing the go-around – CODE: COM" (see excerpt in Fig. 2), it is translated into an indicator belonging to "Communication and coordination" (as highlighted by blue box in the excerpt in Fig. 3). However, it can play a role in other linked patterns of the sheet, such as "Cross-scale interactions" and "Timing and synchronization".

Consequently, once the recorded ATC contributing elements have been translated into some resilience patterns/indicators, they can be linked between them and with the capabilities. The drawn connections cause for reflection on interrelations, impacts and performance variability.

Through this illustrative example, we have explained in detail as the protocol and the supporting material described in "2 OBSERVING RESILIENCE: A PROTOCOL" can be applied in practice.

Fig. 4 shows the protocol in use, the supporting material needed for each step and the related output.

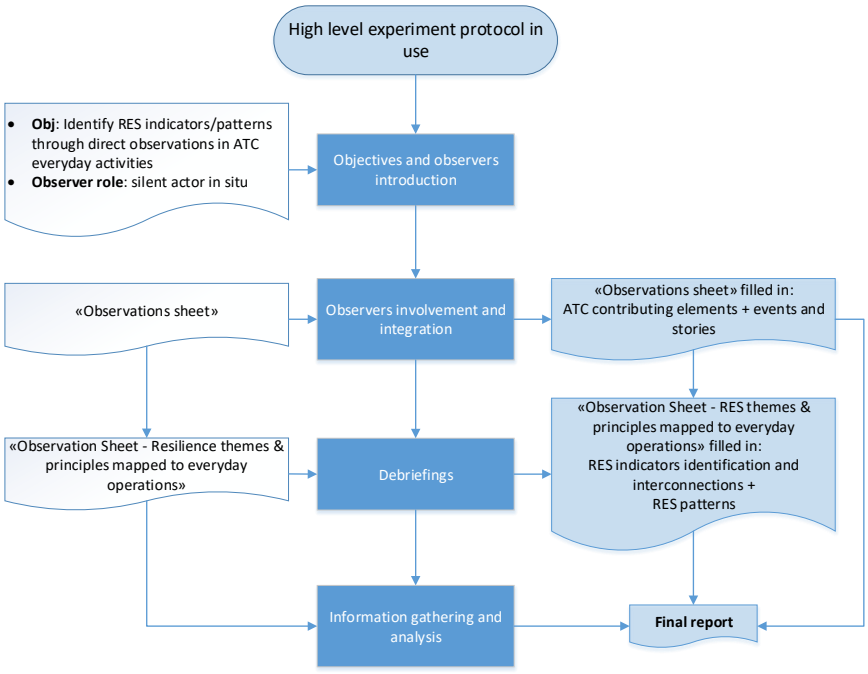


Figure 4. High-level experiment protocol in use, supporting materials and outputs

3 PRELIMINARY FINDINGS AND NEXT STEPS

This paper has presented a protocol for observing resilience in practice through direct observations of everyday activities. This has been thoroughly applied on the missed approach procedure, in particular on the go-around manoeuvre. The protocol and the supporting material presented in the paper represent a first step and the results are preliminary. However, from their application in the SCALES project, we conclude that they add significant value when observing resilience in daily activities and to promote a proactive approach.

Nowadays managing resilience is the result of lessons learnt from the past and their adaptation to todays' needs. Be adaptable and act proactively means to deal with the Socio-Technical Systems inborn performance variability. This requires not only speculative effort but also a practical, concrete and daily commitment in order to maintain and improve safety looking at what goes right and at what should have gone right. Theories, models, and methods aim to describe how things go right, but sometimes fail, and how to cope with intractability and unpredictability.

Direct observations can support in understanding how humans behave for adapting and dealing with situations where normal performance variability may combine to create unwanted effects.

In addition, the approach stimulates exchange of knowledge promoting the collaboration between operational staff and scientific community. The different perspectives offered by these complementary stakeholders can ensure a complete and concrete view of the system under analysis. Moreover, this fertile collaboration can support in identifying and analysing resilience patterns and related indicators. These can be used as early warnings to understand the status of the system and act timely in order to anticipate and prevent negative outcomes.

The proposed approach and these preliminary patterns/indicators can be used as example for continuing Resilience Engineering research in everyday activities in order to improve both these preliminary findings but also to investigate other ones.

Currently, the protocol has been applied only in the Air Traffic Management domain for observing resilience in different ATCs such as Fiumicino (FCO) and Ciampino (CIA) in Italy and Trondheim-Værnes (TRD) in Norway. However, thanks to its flexibility and customization, it can be adopted in different application domains.

Acknowledgements

The SCALES project is co-financed by EUROCONTROL acting on behalf of the SESAR Joint Undertaking (the SJU) and the EUROPEAN UNION as part of Work Package E in the SESAR Programme. Opinions expressed in this work reflect the authors' views only and EUROCONTROL and/or the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

REFERENCES

Blomberg, J., Burrell, M. (2009). An ethnographic approach to design. *Human-computer interaction: Development process*, 71-94.

Federal Aviation Administration (FAA) (2014). Aeronautical Information Manual. https://www.faa.gov/air_traffic/publications/media/AIM_Basic_4-03-14.pdf, accessed on 12-05-15

Hayes, J. (2013). *Operational decision-making in high hazard organizations, drawing a line in the sand*. Farhnam, Ashgate.

Herrera, I. A., Pasquini, A., Ragosta, M., Vennesland, A. (2014a). *SCALES D2.1 – Case studies description*. Edition 00.01.01 (under SJU approval).

Herrera, I. A., Pasquini, A., Ragosta, M., Vennesland, A. (2014). *The SCALES framework for identifying and extracting resilience related indicators: preliminary findings of a go-around case study*. 4th SESAR Innovation Days, Universidad Politécnica de Madrid, Spain, 25th - 27th November 2014.

Herrera, I. A., Pasquini, A., Ragosta, M., Vennesland, A. *Resilience view and practical indicators* (incoming paper)

Hollnagel, E. (2008). *From protection to resilience: Changing views on how to achieve safety*. 8th International Symposium of the Australian Aviation Psychology Association, Sydney, Australia.

Adapting to the unexpected in the cockpit

Rogier Woltjer [1], Joris Field [2], and Amy Rankin [1]

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

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

[2] National Aerospace Laboratory NLR, Amsterdam, the Netherlands

[2] joris.field@nlr.nl

http://www.man4gen.eu/

Abstract

This paper reports a flight simulation study where airline flight crews were tasked to handle unexpected situations as part of the "Manual Operations for 4th Generation Airliners" (Man4Gen) EU FP7 research project. The analysis of 12 flight crews as crew-automation Joint Cognitive Systems combined a cognitive systems engineering perspective with debriefing methods focused on sensemaking. Two central themes emerge from the combined analysis of control strategies and sensemaking in the crew-automation JCS that are of relevance to Resilience Engineering and to further the understanding of how crew-automation systems adapt to unexpected situations. First, the results point to the importance for operators of understanding time available their ability to "create" available time. This was found in our analyses of debriefing and modelling of how control loops with different time horizons interact (ECOM). Second, both analyses highlight how the common understanding of goals and priorities, and assessing risks and opportunities aid in coping with the unexpected.

1 INTRODUCTION

Modern civil aviation has become an extremely safe mode of transport, an accomplishment that can be largely attributed to the application of reliable and advanced aircraft systems. Despite the high degree of automation found in all aircraft systems, ranging from fuel control to flight control, the flight crew remains responsible for the operation of the aircraft. In the rare circumstances that automation fails, the crew may be faced with (several) unexpected situations and are then expected to respond appropriately. The "Manual Operations for 4th Generation Airliners" (Man4Gen) EU FP7 research project is investigating the risk assessment and decision making strategies applied by flight crews facing an unexpected situation in a modern airliner (see www.man4gen.eu). The project aims to contribute to short-term recommendations to the aviation community, to increase the overall resilience of the crew-aircraft system (Field & Lemmers, 2014). Techniques and concepts from Cognitive Systems Engineering (CSE) related to Resilience Engineering (RE) are applied to investigate and better understand the actions, behavioural patterns and strategies of the flight crew-aircraft Joint Cognitive System (JCS).

The research question investigated in this paper is: How do flight crew recognise unexpected threats and which strategies do they apply to anticipate their consequences, monitor their development, and respond?

We report the results of an experiment that was carried out in a research flight simulator, where 12 flight crews were subjected to a scenario with three unexpected events. The analysis described in this paper combines a CSE (Rankin, Woltjer, Field, & Woods, 2013) and sensemaking perspective (Klein, Phillips, Rall, & Peluso, 2007; Weick, Sutcliffe, & Obstfeld, 2005), to examine the actions and decisions of the flight crew and identify the strategies that are applied when adapting to the situations and events in the simulator. This descriptive analysis of the crew's decisions and actions is combined with the results of an industry derived analysis of the crew's performance.

2 BACKGROUND

CSE sets out to investigate the ways in which people work within the applicable context for the work; the flight crew operating in the flight deck in this case. Studying work practice in an operational setting warrants the main contextual factors to be included in the analysis; factors such as the influence of organizational, as well as cognitive and situational demands (Woods & Hollnagel, 2006). By examining crew behaviour in a simulated operational setting, the identification of interactions between the crew members, as well as with the aircraft and systems are included in the analysis. Within CSE, both people and technical systems are considered as elements collaborating as a JCS, which enables an analysis of how the humans and systems function together. CSE methods analyse the

behaviour of this JCS to describe the patterns and characteristics of observable behaviour (Hollnagel & Woods, 2005). In the experiment described here we consider both pilots – Pilot Flying (PF) and Pilot Monitoring (PM) – along with the aircraft automation and systems, as the JCS.

At the core of the CSE perspective is the relationship between joint cognitive systems and their environment, which can be illustrated by both ECOM and the Contextual Control Model (COCOM) sensemaking and control loop (Hollnagel & Woods, 2005; Rankin, Woltjer, Field & Woods, 2013). COCOM and ECOM models have been applied in the analysis of human-machine systems – in aviation and beyond (e.g., Feigh, 2010; Kontogiannis & Malakis, 2011). Rankin, Woltjer, Field & Woods (2013) described how COCOM can be applied within the crew-aircraft JCS context. The knowledge and experience of the flight crew form the basis of the interpretation of a situation the crew encounters. Their understanding of the situation is built up from interacting with the cockpit displays and interfaces, as well as the physical cues (noise, vibrations) from the aircraft. This understanding is what the crew's actions and decisions are based on. Their actions, combined with external events, yield feedback which modifies the understanding, forming a perception and action loop.

The ECOM (Hollnagel & Woods, 2005) is a model to describe multiple layers of performance of the joint crew-aircraft system (illustrated in **Figure 5**). This functional model can be used to examine the distribution of tasks and roles across the different crew members and aircraft systems. Several layers of control loops are applied to describe how anticipatory (feedforward) and reactive (feedback) control are performed simultaneously by the system. As a situation unfolds the distribution of tasks and roles may change and the focus and attention of the crew may shift, demonstrating how the crew-aircraft system adjusts to respond to an event.

This functional account of the joint system recognizes that a systems performance takes place simultaneously on multiple layers of control (**Figure 5**). The four layers of interacting control loops in the ECOM thus describe how a JCS set targets (e.g., "heading for destination"), plans (e.g., "monitor flight path"), regulates (e.g., "reduce speed ahead") and track performance (e.g., "adjust speed"). The goals set at the targeting layer provide inputs and targets for the planning, regulating and tracking layers and reversely the tracking layer provides input to revision of goals and targets. The simultaneous anticipatory (feedforward) and reactive (feedback) control is shaped by the current conditions and system constraints.

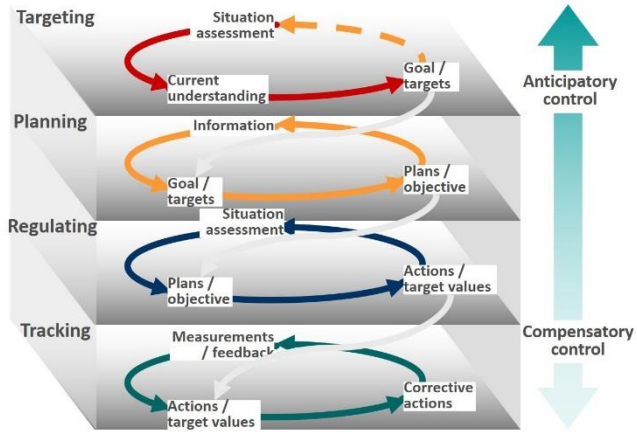
Extended Control Model (ECOM)	Layer	Activities in flight context
	Targeting	Setting and resetting high-level goals of what may happen in the future
	Planning	Carry out monitoring and planning actions, where is the A/C going to be and how it is going to get there.
	Regulating	Executing the tasks as part of the plan that has been put together in the planning layer.
	Tracking	Actions that have a direct impact on the A/C control surfaces, direct effect on the A/C behaviour

Figure 5. *The Extended Control Model (Hollnagel & Woods, 2005) with activities described in a flight context*

In this simulator experiment we aim to investigate how crews adapt their performance to cope with unexpected situations. The research focus is on understanding the sensemaking and control processes taking place. The combined Cognitive Systems Engineering (CSE) and sensemaking approach resulted in the following research questions that are also central questions in Resilience Engineering:

- How do flight crew recognise unexpected threats and which strategies do they apply to anticipate their consequences, monitor their development, and respond?
    - How do crews search for information, manage uncertainties, prioritise and make trade-offs, assess risks, consider options and anticipate future events, in order to anticipate, monitor, and cope with unexpected situations?
    - How can strategies or patterns be identified regarding anticipation, monitoring, and response?

The CSE perspective of the analysis is applied using the Extended Control Model (ECOM; Hollnagel & Woods, 2005), which identifies the crew's actions in different layers of control (targeting, planning, regulating and tracking) to

examine crew strategies to adapt to unexpected situations. The analysis aims to understand the performance of the crew-automation JCS (Hollnagel & Woods, 2005) and what this means for the crew's ability to anticipate, monitor and respond to events effectively, relating to three of the four cornerstones of resilience (Hollnagel, 2011). The aim is to describe and explain the variability in performance, and to learn from the simulation's results in terms of training and instruction, and other operational recommendations such as crew collaboration and use of procedures.

3 METHOD

The experiment applied an operationally relevant situation for trained line pilots, and aimed to investigate how the crew deals with unexpected situations. It was of particular interest to study the crews' risk assessment and decision making. The scenario included events that crews were unlikely to have encountered during routine training, which were designed to address the main project goals: automation failure and reversion to manual control; an event that required authoritative decision making; a challenging and ambiguous situation.

The experiment was carried out with a total of 12 crews of line pilots, both captains and first officers – a total of 24 pilots. All crew members were active line pilots or recently retired. Crews were unaware of the events in the scenario, and were instructed to treat the scenario as a normal operational flight. The NLR's "GRACE" research simulator was used for the experiment; the flight deck was set-up in a Boeing 747-400 configuration.

The experimental scenario was developed by operational experts within the consortium including representatives from aircraft manufacturers, operators and training organisations. The scenario focused on the final descent and approach phase to an airfield, after a long-haul flight. Three key events in the scenario formed the unexpected situations that were being studied. The first occurred during the final approach to the runway – an increase and shift in the wind, destabilising the approach path leading to a go-around. An additional loss of visibility at the decision height would force a go-around if necessary. During the go-around, the second event occurred, which was a subtle failure of the autopilot heading control that would necessitate a reversion to manual control to regain control of the aircraft heading. The third event was a birdstrike during the go-around climb-out that caused a failure of engine 1, and damage to engines 3 and 4. The damaged engines would surge and stall until thrust was reduced on those engines, at which point the aircraft could be stabilised. The crews were free to decide the appropriate response to the failures, and to decide on the course of action – for example returning to the airfield for a landing, or stabilising the aircraft and diagnosing the problems before landing.

The research simulator was set up to record data for the analysis of the flight crew's actions, decisions and behaviour, including simulator log data, audio and video recordings. At the end of the experimental scenario, the flight crew were debriefed by the project researchers. Recordings of the debriefings were transcribed, and contributed to the analysis. The crew's communication and actions were captured during the analysis by transcribing the video and audio recordings.

The data used in the COCOM/ECOM analysis presented in this paper consisted primarily of the observation log, video data (of the cockpit, flight crew and displays), and audio recordings from the flight deck and debriefing interviews. Performance of the crews related to expected actions and decisions was examined by three industry experts, determining which desirable actions (from a flight safety perspective) were performed.

3.1 COCOM/ECOM

For the description of the degree and kind of control that the crew-aircraft JCS displayed during the simulator session, the COCOM and ECOM models were translated to an operational context for classification of the observations from the experiment. The ECOM was used to classify the behavioural patterns (see also Field, Rankin, & Woltjer, 2014), and the COCOM was applied to assess the degree of control.

To operationalise the ECOM, the four layers - Targeting, Planning (originally called Monitoring), Regulating and Tracking - were applied to the experimental data and context of the crew-aircraft JCS, as described in **Figure 5**. Assigning the observations to the different layers was done through an iterative process of classifying the observations based on the theoretical descriptions of the ECOM model (Hollnagel & Woods, 2005). Dataset from two crews were used to develop the initial classification scheme using three independent raters. This classification scheme was documented and extended, iteratively reaching full inter-rater consensus while being applied to the remaining datasets. The patterns of activities were classified according to the four ECOM layers for a selection of flight phases/segments and crews: Engine management (after birdstrike); Trajectory management (second approach after Go-Around) to landing; and Manual reversion (after HDG failure).

The COCOM classification scheme describes the degree of control that the crew-aircraft JCS has in a specific time period of performance. A classification of the control mode (strategic, tactical, opportunistic, scrambled) per flight phase was made using the literature definitions proposed by Hollnagel & Woods (2005), based on three

parameters: (i) subjectively available time; (ii) evaluation of outcome, and (iii) selection of action. These were assessed by two of the project researchers that also performed the ECOM classification.

3.2 Debriefing

The debriefings were applied after the experiment and were carried out in two stages: (a) individual debriefings (PF and PM separately), and (b) a joint debriefing (PF and PM together). The individual debriefings (PF and PM) were carried out directly after the flight. This debriefing took 5-10 minutes and included a standard set of questions asking the crew members to recall what happened after the go-around, what options and priorities they considered and what risks they identified. In the joint debriefing the crew members together watched a replay of the video recording of the flown scenario. The video was played from just before the go-around until landing. The de-brief facilitator and the crew members could stop the video recording at any time to discuss the crew's performance. This video debriefing took approximately 30-45 minutes.

At first the data from the audio recordings from the three debriefings was transcribed and summarized along the main events and topics of interest in the scenario. In a next step summaries from the two individual (PF and PM) and the joint debriefing per crew were compiled into one summary. This also included a comment if there were any differences in answers between the de-brief sessions. Next the data was tagged per major flight event or flight phase, according to theoretical concepts in CSE/sensemaking theory. After the data was tagged the analysis was structured so that comparisons between crew members and between crews could be carried out. Given the large amount of data acquired research topics of particular interest were chosen as a means to search for patterns. These topics were based on the theoretical concepts of sensemaking.

4 RESULTS AND ANALYSIS

4.1 COCOM/ECOM

This paper reports the engine management (after the bird strike) analysis, and focuses on the broadest variability of performance between the crews – using 9 of the 12 crews to illustrate the differences - the top 4 and bottom 5 performers (as rated by the industry experts). The ECOM classification was used to identify patterns of observed performance within the ECOM layers. Then the subjectively available time, kind of evaluation of information, and what information was used for the basis of decision and action were assessed, from which a COCOM control mode was identified. The industry expert ratings of the crew performance were related to the ECOM and COCOM results in the sensemaking analysis, as a rough indication of how the crew performed against the key actions expected for specific moments in the scenario. These 9 crews illustrate a description of the ECOM control strategy and COCOM control mode for the activity of engine management after the bird strike, i.e. stabilizing the damaged engines in order to maximize and balance thrust. Results are illustrated in Table 2. The engine management activity is to a large extent concurrent to the activity of trajectory management mentioned earlier, thus, prioritization that the crews did between the two activities was included in the analysis of control modes. For a more elaborate description of this analysis and the trajectory management results, see (Field, Woltjer, Rankin, & Mulder, 2015).

Table 2. Analysis results for engine management assessment and decisions, in order of number of desired actions performed

Crew	ECOM pattern	COCOM control mode
6	Evaluation, action, evaluation, action, recap	Tactical / strategic
1	Evaluation, action, evaluation, action	Tactical
8	Quick actions, little discussion, evaluation of status, priority	Opportunistic
10	Identify, act, evaluate	Strategic (tactical)
4	Evaluate, prioritizing actions	Opportunistic > scrambled
2	Identify, discussion, action	Opportunistic (tactical)
5	Discussion and inaction	Scrambled /opportunistic
11	Unsynchronized discussion analysis and action	Opportunistic
12	Immediate action, less evaluation	(Opportunistic) > scrambled

4.2 Debriefing

The analysis of the debriefing for all 12 of the crews in the NLR experiment was studied to identify the strategies used by the crews. One of the most relevant results from the sensemaking study of the debriefing was that there were different assessments and priorities of weather and runway options between pilot flying (PF) and pilot monitoring (PM).

In 10 out of 11 crews for which this data was collected (one crew's data was not recorded) the PF and PM made a different assessment regarding the weather and runway options. For example, in 4 crews the difference was whether they should land as soon as possible or take more time to assess the situation. Two crews were focused on different risks, one more concerned about visibility and the other more concerned about the wind. Two crews considered different runways, but did not verbalise this. Two crews agreed on the runway option, but one crew member was a lot more concerned about visibility than the other.

Another relevant result from a Resilience Engineering perspective regards the engine assessment/management, the procedures considered and used, and the variability in crews managing to stabilize the damaged engines. Out of the 12 crews, 7 used the "multiple engine failure" procedure and 5 used the "engine surge and stall" procedure. Not all crews that used the surge and stall procedure managed to stabilize the engines. The focus of the engine failure procedure is shutting down and restarting the engines affected, where the surge and stall procedure focuses on stabilising the engines – the latter is more desirable at low altitudes. There were 3 crews that used the multiple engine failure procedure initially, then later managed to stabilize the engines. For all crews that applied the surge and stall procedure there was a discrepancy in risk assessment and priorities between the PM and PF. In 5 out of 6 crews where the PF called for engine surge and stall, the PM did not agree with this procedure as stated during debriefing (but did not verbalise this during the flight). In 3 of these crews the PM carried out the surge and stall procedures after identifying that the multiple engine failure procedure did not improve the situation. For the remaining crews (who did not manage to stabilize the engines), the PM either did not take action or suggested reducing thrust but did not receive a response from the PF.

Thus, regarding weather and runway options, and the management of the engines, which were critical aspects of the scenario, differences in assessment and priorities by the crew members were reported during debriefing. These differences were in most cases not verbalized during the flight.

There were 4 out of 10 crews (for which clear data on auto-pilot use and reasons to do so was available) that tried to re-engage the autopilot following the bird strike, but reverted back to manual control due to the autopilot failure (with the exception of one crew). Reasons described in the debriefing to re-engage the autopilot were to allow more time to assess the situation, such as the engine state, where to land, and communicate with the PM. However, once re-engaged the autopilot was seen as a distraction by some crews as it was not fully functional. Crews that did not re-engage the autopilot did so because they didn't think the autopilot could cope with the faulty engines, or that they felt more in control and secure when in manual control.

5 Discussion and conclusions

The strategies applied by the crews that performed better with respect to the industry performance assessment of their decisions and actions included interactions between the ECOM layers of Targeting, Planning, Regulating and Tracking. Most activities are triggered as part of procedures or checklists at the planning layer and then subsequently discussed between the crew at the regulating layer; decisions for actions are made, and finally implemented at the regulating and/or tracking layers. If, on the basis of feedback and evaluation, minor adjustments need to be made by the crew to the execution of the plan; this is then done at the regulating layer. If the trajectory needs to be changed to reach the same goal of the flight, these "flight plan" changes are discussed and decided at the planning layer, while higher level goals and prioritization (e.g., runway, alternate airport) is done at the targeting layer. Thus, if there is a regular and frequent interaction between the activities at the various layers of control, performance tends to be of a better quality. For these complex events crews are required to act simultaneously at multiple layers, determining strategies for multiple activities.

The ECOM layers analysis shows that crews with less desirable performance tend to have difficulties in the follow-through and follow-up in the interactions between the layers. For example, if planning decisions and observations are not lifted to the targeting layer when necessary, important considerations regarding choice of runway, and consideration of alternate, and other trade-offs and prioritization of goals may be disregarded. This in turn may lead to lower-layer activities that could be better adjusted to the circumstances if they would be evaluated and reoriented by higher-layer activities, but instead continue to execute plans that are not well-adjusted to circumstances.

Additionally, we have identified that in assessing the situation of the aircraft after an unexpected situation, the flight crew did not all opt for the same procedure – indeed there were often differences between the assessment

of the PF and the PM. Once crews identified a procedure to carry out, there was still variation in the way that the procedure was applied and how it affected the outcome of the flight from the perspective of the industry performance ratings of safety. Both the COCOM/ECOM and debriefing analyses' results support the argument that flight crew had difficulties when facing the unexpected situations in the experiment.

At least two central themes emerge from the combined analysis of control strategies and sensemaking in the crew-automation JCS that are of relevance to Resilience Engineering and to further the understanding of how crew-automation systems adapt to unexpected situations. First, the results point to the importance for operators of understanding time available their ability to "create" available time. This was found in our analyses of debriefing and modelling of how control loops with different time horizons interact (ECOM). Second, both analyses highlight how the common understanding of goals and priorities, and assessing risks and opportunities aid in coping with the unexpected. The CSE analysis and sensemaking debriefing analysis have been used as methods to identify variability among crews. Our results would warrant further research in Resilience Engineering into these themes as typically these subjects don't receive as much attention in the literature as more classical aviation human factors themes.

Acknowledgements

The authors would like to thank the flight crews and experts that participated in the experiment. The Man4Gen research is 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 do not necessarily represent the position and opinions of the Man4Gen consortium and/or any of the individual partner organisations. If you have any questions on the project, please contact man4gen@nlr.nl.

REFERENCES

Feigh, K. M. (2010). Incorporating multiple patterns of activity into the design of cognitive work support systems. *Cognition, Technology & Work, 13*(4), 259–279.

Field, J. & Lemmers, A., (2014) Man4Gen: Manual Operation of 4th Generation Airliners. In *Proceedings of the 31st Conference of the European Association of Aviation Psychology*. Valletta, Malta: EAAP.

Field, J. Rankin, A. & Woltjer, R. (2014). Modelling Flight Crew Strategies in Unexpected Events: A Cognitive Systems Engineering Perspective. In *Proceedings of the 31st Conference of the European Association of Aviation Psychology*. Valletta, Malta: EAAP.

Field, J., Woltjer, R., Rankin, A., & Mulder, M. (2015). Experimental investigation of flight crew strategies in handling unexpected events. In *Proceedings of the 18th International Symposium on Aviation Psychology*. Dayton, OH: Wright State University.

Hollnagel, E. (2011). Epilogue: RAG – The Resilience Analysis Grid. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), *Resilience Engineering in Practice: A Guidebook* (pp. 275–296). Aldershot, UK: Ashgate.

Hollnagel, E., & Woods, D. D. (2005). *Joint cognitive systems: Foundations of cognitive systems engineering*. Boca Raton, FL: CRC Press/Taylor & Francis.

Klein, G., Phillips, J. K., Rall, E., & Peluso, D. A. (2007). A Data-Frame Theory of Sensemaking. In R. R. Hoffman (Ed.), *Expertise out of context* (pp. 113–155). New York, NJ: Lawrence Erlbaum Associates.

Kontogiannis, T., & Malakis, S. (2011). Strategies in controlling, coordinating and adapting performance in air traffic control: modelling "loss of control" events. *Cognition, Technology & Work, 15*(2), 153–169.

Rankin, A., Woltjer, R., Field, J., & Woods, D. (2013). "Staying ahead of the aircraft" and Managing Surprise in Modern Airliners. In I. Herrera, J. M. Schraagen, J. Van der Vorm, & D. Woods (Eds.), *Proceedings of the 5th Resilience Engineering Association Symposium* (pp. 209–214). Soesterberg, NL: REA.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science, 16*(4), 409–421.

Woods, D. D., & Hollnagel, E. (2006). *Joint cognitive systems: Patterns in cognitive systems engineering*. Boca Raton, FL: CRC Press/Taylor & Francis.

ENHANCING RESILIENCE BY INTRODUCING A HUMAN PERFORMANCE PROGRAM

Kaupo Viitanen[1], Christer Axelsson[2], Rossella Bisio[3], Pia Oedewald[1] and Ann Britt Skjerve[3]
[1] VTT Technical Research Centre of Finland, P.O. Box 1000, FI-02044 VTT, Espoo, Finland
[2] Vattenfall AB, Sweden
[3] Institute for Energy Technology, Norway
kaupo.viitanen@vtt.fi
+358 40 845 7618
www.vtt.fi

Abstract

In nuclear industry, human performance programs (HPPs) are commonly used to provide practical solutions for addressing human and organisational issues at nuclear facilities. Human performance programs are implemented by formalizing a selection of working practices called human performance tools (HPTs). In this paper we discuss the insights from our case studies carried out in Nordic nuclear power plants and the input received from human performance experts around the world, and reflect the relation of HPPs to system resilience.

Based on the results of our studies we argue that HPPs have the potential to enhance resilience through various mechanisms. These are i.a. improving organisational learning and monitoring, enhancing staff's understanding of the sociotechnical system of a nuclear power plant, developing practices that help managing the unexpected or providing means of training. The HPPs may, however, also have the potential to be detrimental to resilience. If improperly implemented, HPPs may lead to rigidity and "robotic" ways of performing work, which can even cause safety deteoriration. Therefore, an implementatation process that properly considers the role of HPTs in everyday work and is developed in participation with shop-floor staff is crucial for a successful human performance program.

1 INTRODUCTION

Managing human and organisational factors is a key ingredient in maintaining and improving safety in nuclear power plants. Several approaches are used to provide practical solutions for this issue. In recent years, one of the more popular means to address human and organisational factors has been to introduce a human performance program (HPP). HPPs are typically promoted by various umbrella and peer organisations as development programs that improve safety by reducing active errors and strengthening controls (DoE, 2009a). It is proposed that errors can be reduced through anticipation, prevention, catching and recovering, and controls can be strengthened by means such as eliminating latent weaknesses, removing hazards, engineering barriers, developing instructions or procedures and furthering error-prevention through cultural norms (DoE, 2009a). In practice HPPs are introduced by formalizing a selection of various working practices called human performance tools (HPTs; see Table 1) (DoE, 2009b). Even though HPPs also include examples of practices for management, usually HPPs are targeted solely at the sharp end staff.

The validity of the human-error-focused strategy on safety improvement that also serves as a theoretical background for HPPs has been under debate in the scientific community. It has been argued that rigid control and increased amount of limitations complicate or hinder the execution work, sometimes even causing deterioration of safety (Dekker, 2003). A complementary approach to the error-focused strategy has been proposed by the Resilience Engineering tradition. This approach suggests that instead of focusing on minimizing errors and mistakes, one should switch focus to ensuring that activities result in successes under varying conditions (Hollnagel, 2013). In practice this could mean creating and supporting the preconditions that help various actors in an organisation to perform their work in such a way that results in safety. The aim of this paper is to discuss the relation of HPPs and resilience and provide insights based on the material obtained from our previous studies (Oedewald et al., 2014; Oedewald, Skjerve, Axelsson, Viitanen, & Bisio, 2015; Skjerve & Axelsson, 2014). Our main argument is that even though the explicit rationale underlying HPPs follows a rather error-focused view of safety, due to the adaptive and contextual nature of the HPTs ranging from prescriptive to sensitizing to unexpected situations, HPPs may in practice function as positive, resilience-enhancing programs for working practices.

Table 1. Commonly adopted HPTs grouped by the level of prescription (Skjerve & Axelsson, 2014)

Human performance tool	Description
Promoting adherence to procedures or instructions	
Procedure use and adherence	reducing unwanted events by using and adhering to procedures
Catching errors	
Clear communication techniques (e.g. three-way communication and phonetic alphabet)	means of avoiding misunderstanding in communication
Peer-checking	a pair work technique where one worker observes while another performs the task
Independent verification	an independent worker verifies the task result after completion
Sharing insights and experiences	
Pre-job briefing	a meeting during which all involved prepare for the work task
Post-job review	a meeting during which a completed task is discussed
Task observation	reviewing the quality and effectiveness of tasks by management
Use of operating experience	improving the way in which work is conducted by implementing operating experience programs
Sensitizing to unexpected states or events	
Self-checking (a.k.a. STAR-principle)	a method of boosting attention while performing a task (includes steps of Stop-Think-Act-Review)
Questioning attitude	fostering of uncertainty awareness

HPTs are a heterogeneous variety of working practices that range from simple aids used by an individual to resource-heavy meetings held by a group of people. Even though HPP programs are typically promoted with an error-prevention focus, HPTs may also address several other functions. Four general groups of HPT functions have been identified based on their level of prescription (Skjerve & Axelsson, 2014). The four groups are promoting adherence to procedures or instructions, catching errors, sharing insights and experiences, and sensitizing to unexpected states or events (Table 1). These functions can be further elaborated by considering how they relate to balancing flexibility and rule-based control of work (Grote, 2006; Grote, Weichbrodt, Günter, Zala-Mezö, & Künzle, 2009). Tools at the prescriptive end of the continuum are more geared towards minimizing uncertainty and promoting rigid, non-adaptive working practices. The other end on the other hand can be seen to support coping with uncertainty. Some HPTs fall in between of these extremes (e.g. pre-job briefing and post-job review) and can be seen to have the potential to have aspects of both coping with and minimizing uncertainty. It is argued that both minimizing and coping with uncertainty approaches are required for sustaining resilience (Grote, 2006), which suggests that depending on their contextual application, HTPs from all categories may be beneficial for resilience. HPTs may also contribute to system resilience by addressing Resilience Engineering cornerstones (Pariès, Hollnagel, Wreathall, & Woods, 2012). For example, pre-job briefing may provide support for anticipation and responding, and post-job review can have the function of furthering organisational learning (i.e. the change in organisation's knowledge as a function of experience; Argote, 2013). We argue that the most relevant HPTs to system resilience are those that have the potential of furthering sharing of insights and sensitizing to unexpected events, but also that the use of the more prescriptive HPTs may be beneficial for system resilience when a situation calls for such approaches. The role of the HPP in enhancing resilience would thus be implementing the HPTs in such a manner that the real use of the tools is suitable in a given context and would contribute to reaching desirable goals such as safety.

2 METHODS

The study included three case studies in Nordic nuclear power plant organisations and an international, self-administered web survey (Oedewald et al., 2014, 2015). The case studies were mainly focused on maintenance activities and the international survey was targeted at human performance experts in nuclear industry. The original goal of the studies wasn't to specifically capture or discuss the resilience-enhancing effects of HPPs, but rather to provide general knowledge regarding the impacts and implementation of HPPs.

In two of the three nuclear power plants involved in the case studies a human performance program (HPP) was already implemented. At the third plant there were plans to introduce a HPP, but it hadn't yet been implemented at the time of the study. They were, however, already using some working practices similar to HPTs at the third plant. A total of 47 semi-structured interviews were carried out at the three NPPs. The interviewees represented various levels of management from a variety of different NPP disciplines. This included, for example, maintenance supervisors, technicians, managers and control room operators. The interview questions focused on identifying the expected and experienced benefits and disadvantages of HPPs and what was perceived as important during implementation. In addition to the interviews, in those two plants where a HPP was already implemented, surveys were used to assess personnel opinions regarding the HPP. Data collected from the interviews and the surveys was analysed using a thematic analysis approach (Braun & Clarke, 2006) to identify common patterns and themes.

The international survey was a web questionnaire that was sent to human performance experts in nuclear industry. The individuals were chosen through mailing lists of various human-performance-related seminars and networks. The survey received a total of 87 responses from practitioners at operational plants. All responses were considered in qualitative analyses, and in quantitative analyses only complete responses (n=67) were analysed. Respondents were from at least 47 organisations in at least 13 different countries. Some respondents didn't indicate their organisation or country. The majority of the respondents were from Northern America and the rest were from Europe. The international survey included both open-ended questions and multiple-choice questions. The former were analysed using thematic approach, and the latter were analysed using basic quantitative methods such as statistical means and counts. Open-ended questions concerned expected and experienced benefits and disadvantages of HPPs. Multiple-choice questions concerned the HPTs used, factors driving the introduction of HPPs, indicators used to assess the efficiency of HPPs and key success factors in implementation.

3 RESULTS

Generally the respondents in case study organisations had a positive opinion of the HPPs. They saw that most of the techniques suggested by HPTs have always to some extent been either part of their existing working practices or otherwise desirable good practices. The HPTs were seen useful for i.a. avoiding mistakes, minimizing rework, and making the task smoother and easier to perform. Indirect benefits such as knowledge sharing, organisational learning and safety culture improvements were also mentioned. Many of the respondents didn't find human error a major issue in their work, but instead they discussed problems on practical level such as coordination, preparation or misunderstandings in communication. The human performance expert respondents of the international survey tended consider the error-reduction effects more often than staff at case organisations when discussing the benefits of HPPs. The error reduction paradigm promoted by human performance guidebooks and manuals was clearly reflected in their responses.

Negative responses were mostly related to extra work, cost and time required by some HPTs, relabelling of existing working practices as HPTs or forcefully changing established practices. Many of the respondents also expressed their concern that some HPTs are often used in a rigid way that limits their degrees of freedom in the field and that this may sometimes lead to undesirable outcomes such as causing "robotic" ways of executing tasks or concentrating on executing the tool itself instead of the work task. Respectively, some respondents pointed out the difficulty of deciding how much freedom should be allowed when adapting the HPTs to a particular situation: if too much adaptation by the workers is allowed, HPTs may not be used to the extent expected or in intended ways, and thus the aspect of formalising good working practices may weaken and the HPTs won't be useful anymore.

Pre-job briefing was the most commonly used HPT in all organisations studied. It was implemented in all case organisations (either as a HPT or as a practice) and in all organisations of the international survey. The respondents saw a multitude of benefits to using pre-job briefing: better preparation for work, making sure everyone understands what to do and when to do it, familiarization with the task, coordination between teams and tasks, better understanding of the plant and its functions, education, understanding the connection to other tasks, getting to know all involved etc. The respondents saw that having a pre-job briefing has the potential to both reduce the probability of human error, but also to improve the smoothness of execution, and making the task easier and faster to perform.

Post-job review was usually implemented but it wasn't considered very usable in practice by many respondents. In many cases the respondents perceived it difficult to return back to a completed job tasks to discuss it further unless a clear mistake had been made. Some respondents implied that it could be a cultural issue that a successfully finished task isn't discussed afterwards anymore. Often post-job review was omitted due to practical reasons such as involved workers or contractors having already left the plant after job completion. However, many respondents did acknowledge the potential of post-job review as a learning tool that could facilitate learning and communicating experiences further. Both experiences of errors made and successes identified were considered as something that post-job reviews could help explicate and document.

Self-checking was also one of the most popular tools. This HPT was seen useful by the respondents to identify unexpected situations and to generally avoid engaging in any activities routinely without first considering the specific situation at hand. Unlike the potentially resource-heavy meetings carried out during pre-job briefings and post-job reviews, self-checking was largely perceived as an integrated part of a task's process instead of additional work.

The study revealed that the way HPPs are implemented is critical for the success and usefulness of the program. Such preconditions as proper training, ensuring sufficient resources and integration to existing ways of working and organisational culture emerged. In many responses the negative outcomes were related to a lack of training and integration: the shop-floor personnel were confused on how to use the HPT or why it was important. In addition, the tools were sometimes seen as extraneous or conflicting with their existing work practices or it was unclear whether HTPs are intended to be always used the same way or should they be adapted to the situation. The responses from supervisors pointed out a fundamental issue: there was a degree of confusion or indecision in the management regarding the extent to which the HPTs are allowed to be contextually adapted. Most of the shop-floor staff found that the HPTs can't always be used as such and thus require adaptation. Further confusion and frustration in the shop-floor staff was caused by the mixed messages from management that on one hand required the use HPTs, yet didn't provide sufficient resources for learning or using them. The human performance experts considered that management commitment, training, and managers' activity are the most important key success factors in the implementation of a human performance program.

4 DISCUSSION

HPTs are most often targeted at reducing error of the shop-floor personnel and their potentially system-wide, resilience-enhancing effect isn't usually explicitly discussed. Some of the results of our study imply that HPTs may also have effects on system resilience instead of only affecting sharp-end behaviour. One of these effects is the furthering of organisational learning. The HPTs most obviously related to organisational learning are post-job review and the use of operating experience which can be seen as tools that make the knowledge transfer from the field to the system more efficient. By focusing on those lessons learned that help the system and other sharp-end staff members better face uncertain conditions, these learning tools may be beneficial for sustaining system resilience. Another HTP that has potential to be useful for learning is self-checking, which, if used to sensitize the staff to detect and analyse the unexpected and then bring this knowledge to system level, may enhance resilience through better monitoring of the system state. These HPTs may backfire from resilience point of view if they are used mechanistically or in a simplified manner. For example, if only errors are discussed in post-job reviews, a lot of information (e.g. successful adaptations) that could have the potential to enhance resilience is missed. Error-focused post-job reviews may also foster proceduralization and accumulation of rigid rules. The popular response in the case studies that personnel find it unnecessary to have post-job reviews if everything went according to plans suggests that the post-job reviews in the case organisations were implemented rather as error-collection devices than more general tools for learning. This approach may also reflect the case organisations' cultures in which returning to reflect successful performances aren't seen as beneficial. Similarly, the practical implementation of self-checking usually emphasized boosting the attention of the shop-floor worker to detect errors in their behaviour, rather than furthering learning through identification of good practices or improving monitoring by detecting unknown system deficiencies and then reporting them further. There were, however, examples of cases where an individual staff member successfully handled an unexpected situation due to the use of self-checking.

Another important resilience-related effect that emerged in the studies is the development of an understanding of the system and its sociotechnical components. This is especially related to the pre-job briefing tool. Discussing the related social and technical actors with everyone involved in the task beforehand provides the staff a better understanding of the interconnections of their work to others' and also better understanding of the whole system. In case local adaptations are done, this understanding may help actors make more informed decisions that lead to successful adaptations and thus to more desirable outcomes.

Some human performance experts and top managers related HPPs to improvements of safety culture and general improvements in awareness of human factors in complex sociotechnical systems. These can be interpreted as aggregate effects of all the HPTs and the implementation of the HPP itself. Most often such cultural characteristics as rigour and discipline were mentioned in the responses. However, if the implementation of the HPP is focused on error-reduction and rule-based control, and the implementation process is top-down, it may result in cultural characteristics that are not desirable. Behaviour characterized as "robotic" or staff shifting focus on performing the tools instead of the task may result from improper implementation process. In such case HPTs are used for the sake of compliance without real understanding of their benefits or usefulness and thus the potential positive effect will be reduced.

Finally, the semantics and logics used in the promotional material (incl. training) of HPPs may have an effect on

how they are received in practice. Typically HPPs are presented as methods that result in better safety through error reduction. This argument was popular among the human performance experts. However, when HPTs were applied in the field, the shop-floor staff considered the human error reduction effect rather secondary and emphasized effects such as better understanding of work, improved coordination, smoother and faster execution of work etc. HPTs were perceived as "good, professional working practices" instead of merely error-reduction methods. This may suggest that the shop-floor staff may in fact readily have a better systemic understanding of the relevance and significance of HPPs than human performance experts and management. Shop-floor staff sees the HPTs as more integrated and applicable to other purposes than error reduction as assumed by human performance experts and management. Furthermore, this suggests that if error-reduction is the primary argument used in promotional materials of HPPs or by the top management, the shop-floor staff may find that their expert judgement and experience is not valued or understood which may result in a lack of motivation to use them or in a confrontation between the shop-floor staff and top management. There were strong opinions from some of the shop-floor interviewees that the top management and human performance experts lacked the understanding of the real issues in everyday shop-floor work. This confrontation indicates a problem in communication between the levels of organisation and may also suggest that the management hasn't understood how the HPTs are used in practice or how they will be used in practice. This is especially problematic with experienced workers that are already using practices similar to HPTs because the introduction of HPTs may contradict with their existing practices. This issue further emphasizes that HPPs should be integrated to the organisation as part of continuous work practice and process development, developed in collaboration with the staff, and providing guidance and recommendations for the staff instead of rigidly prescribing their behaviour. Conversely, when viewed from newcomer's perspective, a HPP was seen useful as a training tool. By implementing a HPP, the newcomers are provided a quick and easily understandable reference of how work at a given facility should be performed. Such effect may further organisation's resilience by facilitating the promotion of desirable safety culture.

Based on the insights from our studies, HPPs can be seen to have resilience-enhancing effects under certain conditions. It appears that HPPs have the potential to promote both prescriptive and limiting ways of working but also resilience-enhancing ways of working. The prescriptive effect was reflected in the multitude of responses where concern of limiting staff freedom to adapt locally was expressed – HPTs were perceived as something that inhibit personnel's own judgement or use of professional experience. However, a common response also was that HPTs have had the effect of supporting the work and that better training, use and understanding of such practices during the implementation of a HPP would further improve this effect. This suggests that the manner in which the HPP is implemented plays a crucial role in the resilience-enhancing effect: if the HPP is implemented mainly with a top-down, rule-enforcing control in mind, the HPTs used in a mechanistic way and not much thought is put in making sure the end user understands the actual function of each of the tools, the result might not improve the organisation's resilience, but rather decrease it. On the other hand, if the implementation process acknowledges the role of HPTs as means to improve working practices by supporting workers instead of using prescription to control them, the HPPs may have the potential to enhance resilience.

In summary, three main factors relate to how useful HPPs are to enhancing resilience at nuclear power plants. First, the selection of the HPTs to be implemented needs to be such that resilience-enhancing effects are plausible. The tools that most probably enhance resilience help the end users face the uncertainty at individual level but also carry this ability further to the system level. Examples of such are well-implemented pre-job briefings and post-job reviews. The selection of HPTs shouldn't be limited to the most non-prescriptive ones because depending on context, both prescriptive and non-prescriptive HPTs may be beneficial for resilience. Second, the implementation process needs to be designed in a way that it supports enhancing resilience. If the HPTs are implemented to provide top-down control, add restrictive procedures and limit local adaptations, the beneficial effect of the workers' professional input on task performance may be eliminated. This may lead to instrumental use of HPTs and possibly reduced system resilience. It is to be noted, however, that all variance is not desirable. For example, as discussed by some of the respondents, allowing too much freedom on adopting the HPTs may lead to staff using them incorrectly or not using them all, both of which have the potential to result in negative outcomes. Emphasizing the actual function of the tool and making sure everyone (incl. top management and human performance experts) understands how, when and for what purpose the tools are beneficial are some of the preconditions that need to be met in order for the tools to result in increased resilience. Third, the way in which the HPTs are actually used at shop-floor level needs to be considered. For example, if a HPT, or a similar pre-existing practice is considered helpful in multiple ways depending on the context, the (re)introduction of the HPT as merely an error-reduction method may lead to confusion, a lack of motivation to use the tools, or in worst cases, conflicts between various parties within the organisation. The integration to existing work practices is therefore essential.

5 CONCLUSIONS

Human performance programmes provide a concrete set of tools that are widely applied in real-life situations. They also appear to have potential to be beneficial for creating or sustaining resilience. However, our study also showed that there are a variety of practical issues involved in implementing a successful human performance program. This has implications for enhancing resilience at an organisation - contextual and systemic factors and the implementation process have an important role and need to be considered. Merely developing a variety of methods that in some conditions may enhance resilience doesn't guarantee that the practical implementation of those methods is at all beneficial for resilience. Using HPTs in a rigid and mechanistic may in some cases even result in safety deterioration. Therefore, in addition to choosing well-developed practices, proper implementation process and close collaboration with those who use those methods are crucial in ensuring that the resilience-enhancing effect actually takes place.

Appendix 1. Resilience skills and constraints for electricians and hydroelectric power plant operators (light gray signs means similar RSs)

	Electricians (Wachs et al, 2012)	**Hydroelectric Power Plant Operators**
Resilience Skills	To discuss, with the central operations control room team, procedures to be followed and/or to request information on the network	To coordinate activities with the COGE
	To discuss, with the colleagues who are in the field, to build a shared understanding on the situation	To coordinate activities with the other shift worker
	To discuss, with the consumers and population, the status and hazards of the power line maintenance procedures, as well as the possible causes of defects	
	To express doubts and fears to other team members and request help from them	
		To coordinate activities with maintenance staff
		To coordinate activities with other actors
	To identify structures, lines or equipment that are non-standard, damaged or have failed	
	To identify visible signs in the environment that indicate difficulties in doing the task or the likely causes of damages to the line	
	To draw up strategies to identify defects in the power line	To interpret information from supervisory controllers, equipment or the environment
	To draw up work strategies, after the defects have been identified	To draw up action strategy to reestablish plant operations
	To plan and to check the availability of the equipment and materials that are necessary to undertake the task	
	To distribute the task between team members and to do the task accordingly	
	To identify sources of stress and fatigue	To identify sources of stress and fatigue
	To draw up strategies to cope with stress and fatigue	
		To determine priority actions
		To understand the role of each piece of equipment in the plant's operations
		To recognize the power plant as an interconnected generation system
		To recognize the implications of stopping the generation unit
Constraint	Activity carried out previously, at the same location, in an inadequate way	
	Lack of equipment or materials to undertake the activity	
	Failure in power line equipment or materials	Equipment failure or damage
		Failure of the supervisory control system

	Lifting weights and need to use a lot of physical strength	
	Long working hours	Increased operational workload
		Increased bureaucratic workload
	Lack of support from a colleague	
	Pressure from supervisors, central operations control room or clients	Time pressure
	Problems at the interface between the electricians in the field and the operations center	
	Difficulty of access to the region	
	Difficulty of access to the power line	
	Night	
	Adverse weather conditions	Problems outside the power plant
	Region in turmoil because of urban violence	
	Presence of animals or insects	
actions for redesigning the socio-technical system	Acquiring equipment with greater range to facilitate communication between electricians at the field and among them and the central operations control room	Providing the equipment needed for power plant activities
	Updating the company's maps, especially in terms of street names and characteristics of the network	Implementing a management system for information collected by the ODR (operator driven reliability)
	Providing mobile devices to support lanterns required for night work	Implementing a training and continuous education program for operators
	Re-evaluating and possibly increasing the number of operators in the central operations control room	Developing procedures to ensure operating staff are aware of all the activities performed at the plant
	Training teams to read and interpret maps	Optimizing signals/alarms used in the supervisory control system
	Performing cross-training events between teams of electricians and from central operations control room, so that one party gets to know the reality of the work of the other party better	Carrying our corrective maintenance on equipment
	Expand preventive maintenance actions in the network	Reducing the workload of operators
	Develop standards for communication between field teams and central operations control room	
	Broaden and strengthen the practice of filling a checklist of available materials and tools at the beginning of each shift	
	Improve the distribution of tasks among the different shifts so as to reduce overtime	
	Draw up a formal program for refusing risky tasks	
	Increasing the frequency of inspections to identify constructions next to the power lines, thus detecting situations in which the minimum distances between the lines and buildings is not respected	
	Increasing the frequency of inspections in areas known to have many clandestine connections	
	Conducting public awareness campaigns about the dangers of the power lines and about the dangers of clandestine connections	
	Defining together with other institutions which share the grid (for example, town hall and the secretary for the environment), procedures of use and maintenance	

REFERENCES

Argote, L. (2013). *Organizational Learning*. Boston, MA: Springer US.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77–101.

Dekker, S. (2003). Failure to adapt or adaptations that fail: contrasting models on procedures and safety. *Applied Ergonomics*, 34, 233–238.

DoE (2009a). *Human Performance Improvement Handbook Volume 1: Concepts and Principles*. DOE Standards. Washington, D.C.: U.S. Department of energy.

DoE (2009b). *Human Performance Improvement Handbook Volume 2, Human Performance Tools for Individuals, Work Teams, and Management*. Department of Energy Washington, DC: Government Printing Office.

Grote, G. (2006). Rules management as source for loose coupling in high-risk systems. In *Proc. of the Second Resilience Engineering Symposium* (pp. 116–124).

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, 17–27.

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

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.

Oedewald, P., Skjerve, A. B., Axelsson, C., Viitanen, K., Pietikäinen, E., & Reiman, T. (2014). The expected and experienced benefits of Human performance tools in nuclear power plant maintenance activities - Intermediate report of HUMAX project (No. NKS-300). NKS.

Pariès, M. J., Hollnagel, E., Wreathall, M. J., & Woods, D. D. (2012). *Resilience Engineering in Practice: A Guidebook*. Ashgate Publishing, Ltd.

Skjerve, A. B., & Axelsson, C. (2014). Human-Performance Tools in Maintenance Work - A Case Study in a Nordic Nuclear Power Plant (No. NKS-321). NKS.

REGULATIONS AND RESILIENCE

VIOLATION OR RESILIENCE? A COMPARISON BETWEEN TWO FRAMEWORKS FOR MAKING SENSE OF WORK-AS-DONE

Marcelo Fabiano Costella1, Tarcisio Abreu Saurin2, Fabricio Borges Cambraia3, Heleia Bortolosso4
1, 4 Universidade Comunitária da Região de Chapecó, Av. Atilio Fontana, 591-E, Chapecó, SC, Brazil
2 Federal University of Rio Grande do Sul, Av. Osvaldo Aranha, 99, 5. andar, Porto Alegre, RS, Brazil
3 Universidade Federal de Juiz de Fora, Rua José Lourenço Kelmer, 55, Juiz de Fora, MG, Brazil
1costella@unochapeco.edu.br; Tel: +55-49-9982-4808
2saurin@ufrgs.br
3fabricio.cambraia@engenharia.ufjf.br
4heleia@unochapeco.edu.br

Abstract.
This paper compares two frameworks that help to make sense of work-as-done. One of these frameworks was proposed by Saurin, Costella and Costella (2010), and it allows the identification and classification of types of human error according to the skill-rule-knowledge based structure (Reason, 1997). The other framework was proposed by Rankin et al. (2014), which emphasizes the identification and classification of performance adaptations according to the resilience engineering paradigm. The comparison is illustrated by the analysis of a safety incident related to the work of electricians who perform emergency maintenance on overhead power distribution networks. The type of human error identification framework indicated that there was a violation on the part of workers, while the adaptation analysis framework revealed a resilient action. Although the type of human error identification framework revealed issues related to the quality of procedures, training, and technical failures, it did not provide visibility of resilience aspects and encouraged oversimplified analyses by relying on yes-or-no answers.

1 INTRODUCTION

Deviations from the prescribed work are often treated as violations by accidents investigators and even in academia. From this perspective, deviations occur intentionally and the typical corrective measures involve the reinforcement of training so that people follow rules, disciplinary sanctions and, less frequently, the redesign of the prescribed work. on the other hand, several studies stress the context in which the violations occur. for example, in complex and high-risk environments, such as nuclear power plants, Leveson (2004) found that rule violation seemed to be quite rational when one takes into account the overwork and time pressures under which operators perform their tasks. Violations may in fact be an inevitable by-product of the need to achieve the desired performance in complex systems (Polet; Vanderhaegen; Amalberti, 2003). In this light, violations are not a risk, but rather a reflection of the intelligence and adaptability of workers (Amalberti; Auroy; Aslanidès, 2004).

By contrast, the resilience engineering (RE) view emphasizes the need for the continuous feedback of work procedures so as to minimize the distance between the prescribed and actual work, which tends to reduce the incidence of violations. In fact, RE argues that monitoring and modifying the rules is as, or even more important than their initial development (Hale; Guldenmund; Goossens, 2006). Based on this, organizations should give support to workers so that they can make performance adaptations when necessary (Grøtan et al., 2008). From the RE perspective, therefore, adaptations by workers serve to adjust imperfections in procedures, which will always be incomplete (Sandberg; Albrechtsen, 2014).

This paper discusses how these two perspectives - violations and resilience - can be used to make sense of safety incidents. Two tools that are representative of the two perspectives were chosen to support the analysis: a framework for the identification and classification of human errors (Saurin; Costella; Costella, 2010), and a framework for adaptation analysis (Rankin et al., 2014). Both tools were applied to the analysis of a safety incident related to the work of grid electricians who perform emergency maintenance in an electricity distribution network. This sector was chosen since it has characteristics of complex socio-technical systems, such as uncertainty and a dynamic work environment.

2 THEORETICAL BACKGROUND

2.1 Identification of types of human error

The tool for the identification of types of human error is based on a classification of three levels of cognitive performance proposed by Rasmussen, known as the SRK model. Reason (1997), however, discusses these levels at length. According to this author, the three levels of performance are:

- Skill-based (SB): carrying out routine tasks in an automatic way. This is the mode in which people work most of the time.
- Rule-based (RB): applying memorized or consciously written down routines in order to verify whether the solution is adequate or not.
- Knowledge-based (KB): this is a level in which people enter reluctantly, only as a last resort and in new situations, which applies neither routines nor rules.

The framework for the identification of types of human error was developed on this foundation by Costella and Saurin (2005) based on the observation, in a case study, that accident investigations defined most accidents as being caused by a "lack of attention" of the victims. However, in a more in-depth analysis this did not fit reality, which motivated the development of a tool that could assist in the investigation of accidents and give visibility to the context in which the human error occurred.

The final version of the framework consists of 10 questions (Figure 1), which will be further explained below according to Saurin, Costella and Costella (2010), and which may lead to five types of final answer: slip, lapse in memory, violation, knowledge-based error, and no worker error.

In question 1, the word "task" has a broad meaning, referring to a set of operations carried out to achieve a certain objective. If the answer to question 1 is negative, question 9 should be answered to lead to an end result representing either a violation or the absence of operator error. This part of the framework was introduced because of situations in which the worker was performing tasks outside his usual post.

Subsequently, question 2 should be answered to verify whether the procedure and/or training were appropriate and applicable. If not, the flow chart indicates that the final answer should be "no worker error". If the answer is "yes", on the other hand, then question (3) should be made: "Was the procedure and/or training followed?"

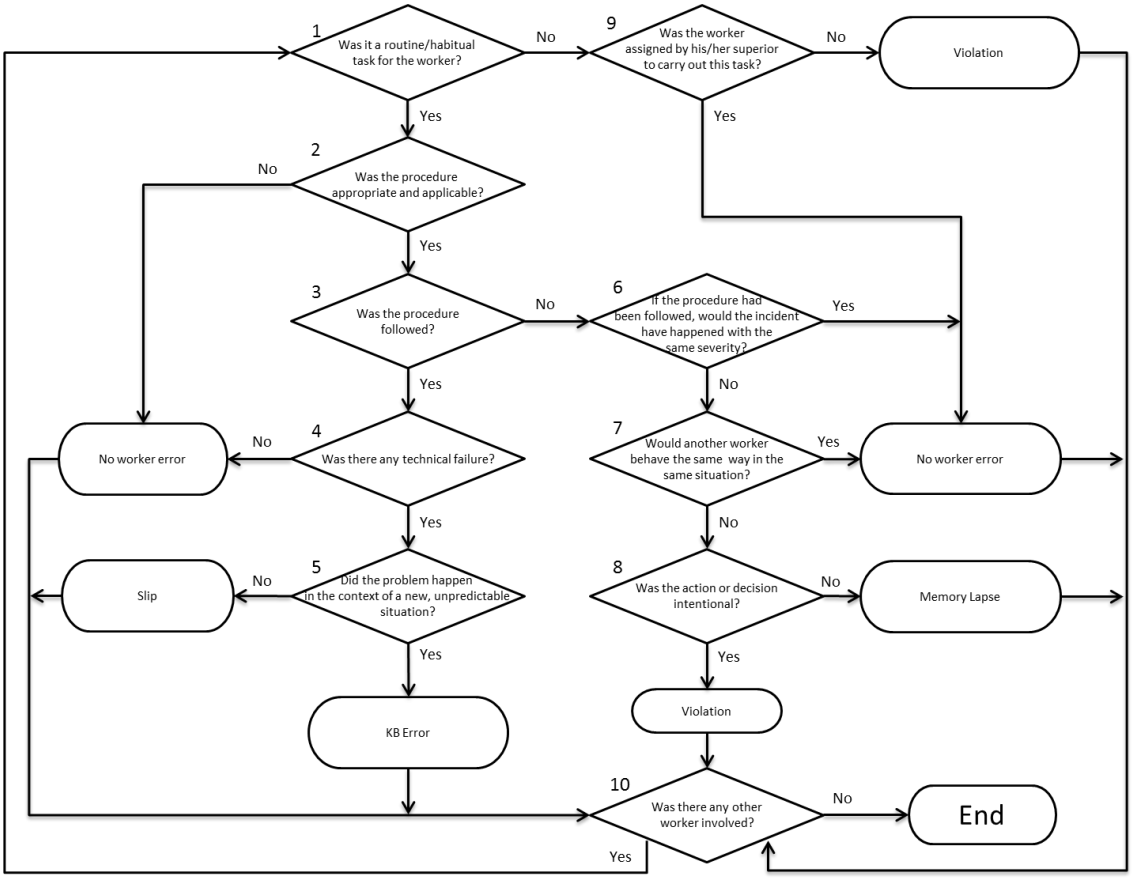


Figure 1. Human error identification framework (Saurin; Costella; Costella, 2010)

This question opens up two large branches in the flow chart. In case of a positive response, one should ask if there was a technical failure (question 4), which, if confirmed, indicates that there was no worker error. If no technical failure occurred, the question whether the problem occurred in the context of an unforeseen situation (question 5) should be asked, which characterizes an error at the level of knowledge (error KB). If it's a routine situation, then the slip is confirmed.

A negative answer to question 3, on the other hand, opens a new branch that starts with question 6. A positive answer to this question indicates that the causes of the event were not linked to either the quality of procedures or the compliance with them, leading to the response "no worker error". In the event of a negative response, question 7 should be asked, which Reason (1997) called the substitution test. If the conclusion is that other workers would have acted in the same way, the chart indicates that the conclusion has to be that "no worker error".

Subsequently, question 8, which asks if the action or decision was intentional or not, will establish if there was a memory lapse. Otherwise, a violation will be registered. It is worth pointing out that after obtaining a conclusion about what type of error occurred, or after concluding that there was no error, one should always question whether other workers were involved (question 10), and if so, run the framework again.

Studies with this framework have been applied in the agricultural equipment sector (Costella; Saurin, 2005), in a fuel distributor (Saurin et al., 2008), in the civil construction sector (Saurin; Costella; Costella, 2010) and in the slaughterhouse sector (Costella; Masson, 2012).

2.2 Framework for the analysis of performance adaptations

Furniss et al. (2011) conducted case studies in the context of a control room of a nuclear power plant in order to observe the strategies used by people during adaptations related to the trade-off between safety and efficiency. To support the analysis of these strategies, a framework was developed that was then perfected by Rankin (2013) and Rankin et al. (2014).

The framework supports the analysis of adaptations performed by workers, targeting three main areas: (a) a contextual analysis, (b) enablers for successful implementation of the strategy, and (c) reverberations of the strategy on the overall system. These three areas are in turn subdivided into:

- Strategy: describes the adaptations used to respond to variation in the environment. “The strategies may be developed and implemented locally (sharp end) or as part of an instruction or procedure enforced by the organization (blunt end) or both (Rankin et al., 2014, p. 6)”.
- Objective: the target for which the adaptation was performed should be described. According to Rankin et al. (2014, p. 6), “the objective is related to identifying demands, pressures, and conflicting goals”.
- Forces and situational conditions: “describes the context in which strategy is carried out (Rankin et al., 2014, p. 6)”. This category helps to make sense of the objectives, which depend on internal and external forces of the organization.
- Resources and enabling conditions: this category describes the existing conditions for the adaptation to be implemented successfully. For Furniss et al. (2011), these conditions may be hard (e.g., availability of a tool) and soft (e.g., availability of knowledge).
- System ability (resilience abilities): the adaptation should refer to one of the four cornerstones of resilience described by Hollnagel (2009), which are, anticipating, monitoring, responding, and learning.
- Sharp-end and blunt-end interactions: first, it is necessary to define at what level the adaptation occurs and how it relates to the sharp/blunt end. In addition, it is necessary to identify how organizational changes affect work performance.

3 RESEARCH METHOD

The study was conducted in an electricity power distributor, which performs works in electrified and un-electrified networks. The study focus was defined as the maintenance procedure of high-voltage electrified networks, given that this was linked to a serious incident detected by the behavior-based safety program, and because it's one of the more complex activities carried out by the company.

In order to understand the real work and obtain data to apply the two frameworks, interviews were carried out with 12 electricians, all male, of which two were shift leaders. The interviews followed a script with twelve questions related to training and procedures – e.g. training and refresher courses, considering the frequency with which they are carried out; whether any of the processes in the procedure are considered unnecessary; whether changes occur in the procedures, how often these occur, and whether such adaptations are re-laid to the safety department and integrated into the working procedures; how each electrician proceeds when the work situation is not covered by a procedure; whether they ever refused a task on duty, and whether they knew that this is provided for in the company's internal rules; whether they consider themselves competent to perform the activities of their profession.

In addition to the interviews, the actual work was observed and documents were analyzed, such as the procedure associated with the incident analyzed and the training records associated with it. This enabled the application of the frameworks and, subsequently, the discussion of the results.

4 RESULTS

The safety incident under study was covered by the maintenance procedure of electrified high voltage networks, which is quite extensive. This procedure covers the repair of the electrical network when something happens that interrupts the supply of electrical power, such as tornadoes, transformer explosions, falling trees, etc. The procedure consists basically of three steps: the stabilization of the pylon(s), after which the cables of the electrical and other existing networks are extended and, subsequently, connected to the pylon and the transformer. This last step is critical since it requires the worker to climb up the pylon.

The procedure studied was the climbing of the pylon, which requires a maneuver to transpose the lower hanging wires, including wires for telephony, cable TV and the low-voltage power network. The most frequent and serious non-compliance with this procedure is related to this transposition, which tends to be adapted by electricians because most of them don't consider the rope grabs coupled to the safety belt to be a reliable piece of equipment. As a result, they perform this transposition by simply fastening the safety belt without the rope grabs. This activity is not safe, because during the transposition, the electrician's safety belt will not be attached. Two fall accidents happened in this company as a result of this situation.

The framework for identifying types of human error, as indicated in Table 1, pointed out that this non-compliance could be classified as a violation, following the response path: 1-2-3-6-7-8-Violation.

Table 1.Human error identification framework paths

N.	Question	Answer
1	Was it a routine/habitual task for the worker?	Yes, all interviewed workers said that they had received training for this task when they joined the company.
2	Was the procedure appropriate and applicable?	Yes, because the procedure is in compliance with national legislation and has appropriate technical principles. They also reported that there is follow-up by a responsible person, who verifies the applicability of the procedure.
3	Was the procedure followed?	No, because they used the safety belt and rope grabs differently than requested. At a given time, while passing the lower cables, they disconnected the belt, which is not allowed.
6	If the procedure had been followed, would the incident have happened with the same severity?	No, since the electrician would not have fallen on the low voltage transition if the safety belt had been fastened to the rope grabs.
7	Would another worker behave the same way in the same situation?	No, because most workers follow the procedure. However the fact that several electricians complained about this step of the procedure indicates compliance can be difficult.
8	Was the action or decision intentional?	Yes, he was aware that they were not following the procedure, since he reported that they felt safer that way.
	Results:	Violation

The application of the adaptation analysis framework (Rankin et al., 2014), on the other hand, produced the following results (Table 2):

Table 2. Adaptation analysis framework paths

Categories	Answer
Strategy	The strategies developed to interpret and respond to changes in the environment were carried out, firstly, by the electricians (sharp end). They also reported that there are adaptations in the procedures and that the written procedures do not occur exactly as the activities in the field, i.e. the sequence of tasks "on paper is one thing, but another in practice". The explanation of electricians is that procedures are created for ideal work situations, but the actual working conditions are rarely ideal, either because of time pressure, failure and/or unavailability of equipment or inadequate planning. The result was that electricians did not trust this piece of equipment and sometimes improvised ways of climbing up the post.
Objective	The objective was to re-establish power in the shortest time possible.
Forces and situational conditions	These are related to the lack of specific training based on the procedure, which is made worse because of the high turnover rate. Furthermore, the field conditions during the execution of the task are often a drawback, since teams could work at night and in the rain.
Resources and enabling conditions	Despite the need for more effective training, there is a formal structure for admission and periodical training.
System ability (resilience abilities)	Responding
Sharp/blunt end	Sharp end, since it is the field teams who respond to the maintenance need.

In summary, the result of the type of human error identification framework was that there was a violation on the part of workers, while the adaptation analysis framework revealed a resilient action. This means that although the type of human error identification framework reveals issues related to the quality of procedures, training, and technical failures, it does not provide visibility of resilience aspects and encourages oversimplified analyses by relying on yes-or-no answers. In fact, this result is consistent with the experience of two authors of this paper who have taught the Saurin, Costella and Costella (2010) framework in undergraduate and graduate courses. Although

it is explained to the students that the framework's purpose isn't to find culprits, and that it should only be the first step or an element of a more comprehensive investigation, many students have difficulty in accepting this recommendation. Terms as "errors" and "violations" tend to be immediately associated with guilt, and the analysis of the event is focused on the negative aspects. The adaptation analysis framework, on the other hand, managed to detect the resilient actions performed by the workers as a result of evaluating six aspects in a descriptive manner, inducing questions that were able to assess resilient actions.

4 CONCLUSIONS

This paper discusses how traditional safety management practices, such as error analysis frameworks, contribute to hiding the adaptive capacity of individuals, teams and organization. This subject was discussed in a highly regulated environment, where non-compliance with procedures occurred as a result of various failures. Most of these were adaptations the workers made during the execution of the work, which, when analyzed through the adaptation analysis framework, could be classified as resilient actions. As such, the two frameworks represent opposing views about the nature of the work in complex socio-technical systems, and it is worth noting that neither completely captures the ambiguity of events. In fact, although the Rankin et al. (2014) framework takes resilience into account, it does not question its side effects, such as hazards that could cause an accident under slightly different conditions.

REFERENCES

Amalberti, R.; Auroy, Y.; Aslanidès, M. (2004). *Understanding violations and boundaries.* The Canadian Healthcare Safety Simposium, 2004, Edmonton, Canadá.

Costella, M. F. ; Masson, R. (2012). *Classificação de tipos de erros humanos: estudo de caso de acidentes em frigoríficos com ocorrências de lapsos de memória.* Encontro Nacional de Engenharia de Produção, 2012, Bento Gonçalves.

Costella, M. F.; Saurin, T. (2005). *Proposta de método para identificação de tipos de erros humanos.* ENEGEP 2005 - Encontro Nacional de Engenharia de Produção, 2005, Porto Alegre.

Furniss, D., Back, J., Blandford, A., Hildebrandt, M.,Broberg, H. (2011). A resilience markers framework for small teams. *Reliability Engineering & System Safety*, v. 96, p. 2-10.

Grøtan, T. O.; Størseth, F.; Rø, M. H.;Skjerve, A. B. (2008). *Resilience, Adaptation and Improvisation – increasing resilience by organising for successful improvisation*. 3th symposium on resilience engineering. Antibes, Juan-Les-Pins, France.

Hale, A. R.; Guldenmund, F., Goossens, L. (2006). Auditing resilience in risk control and safety management systems. In: Hollnagel, E.; Woods, D.; Leveson, N. (Ed.) *Resilience engineering: concepts and precepts.* London: Ashgate. Cap. 18, pp. 270-295.

Hollnagel, E. (2009). The four cornerstones of resilience engineering. In: Hollnagel. E.; Dekker, S. (Eds.) *Resilience engineering perspectives: Vol. 2. Preparation and restoration* (pp. 117-133).Farnham, UK: Ashgate.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science* 42, 237-270.

Polet, P.; Vanderhaegen, F.; Amalberti, R. (2003). Modelling border-line tolerated conditions of use (BTCU) and associated risks. *Safety Science*, v. 41.

Rankin, A. (2013). *Resilience in High Risk Work: Analysing Adaptive Performance*. Licentiate Thesis.Linköping Studies in Science and Technology. Linköping, Sweden.

Rankin, A.; Lundberg, J.; Woltjer, R.; Rollenhagen, C.; Hollnagel, E. (2014). Resilience in everyday operations: a framework for analyzing adaptations in high-risk work. *Journal of Cognitive Engineering and Decision Making*; 8 (78), p. 79-97.

Reason, J. (1997). *Managing the risks of organizational accidents.* Burlington: Ashgate.

Sandberg, E.; Albrechtsen, E. (2014). How to balance between compliance to requirements and safe adaption to situations in the construction industry. In: Steenbergen, P. H. et al. (ed.). *Safety, Reliability and Risk Analysis: Beyond the Horizon.* London: Taylor & Francis Group, p. 1579-1584.

Saurin, T. A.; Costella, M. G.; Costella, M. F. (2010). Improving an algorithm for classifying error types of front-line workers: Insights from a case study in the construction industry. *Safety Science*, v. 48, p. 422-429.

Saurin, T. A.; Guimarães, L. B.; Costella, M. F.; Ballardin, L. (2008). An algorithm for classifying error types of frontline workers based on the SRK framework. *International Journal of Industrial Ergonomics*, v. 38, p. 1067-1077.

INTRODUCING THE CONCEPT OF RESILIENCE INTO MARITIME SAFETY

Jens-Uwe Schröder-Hinrichs[1], Gesa Praetorius, Armando Graziano, Aditi Kataria, Michael Baldauf

Maritime Risk and System Safety (MaRiSa) Research Group,

World Maritime University, P.O. Box 500, 201 24 Malmö, Sweden

[1] jus@wmu.se

http://marisa.wmu.se

Abstract

The maritime industry is still characterized by prescriptive standards and reactive approaches in relation to safety and risk management to a large extent. For a very long time, responses to maritime accidents have been in terms of automation, regulation and training. While this as such is not wrong, it does not offer the full potential that concepts of resilience seem to suggest. The typical question that is predominately asked is still why things go wrong when accidents occur and search for causes and explanations is undertaken. An evaluation of the safety level achieved system and a focus on system components and characteristics that help the system to usually perform safe is typically not part of the investigation. This creates a need to review the current ideas about safety regulations and risk management in the maritime industry as they have probably reached a limit of what they were able to achieve. The concept of resilience engineering with its focus on system performance rather that system failure is a promising concept to be considered in the shipping business, but needs further investigation.

1` INTRODUCTION

The maritime industry is characterized by prescriptive standards and reactive approaches in relation to safety and risk management (Schröder-Hinrichs et al., 2013). Maritime safety standards have traditionally focused on the design of ships and the equipment to be used for shipboard operations. Efforts to improve safety have therefore often addressed specific areas and aspects of ship design and operation, such as stability measures, but not addressing the ship as a socio-technical system (STS) and the organisational context of operations, including the impact of the flag or port state. However, at the end of the 1980s it was realized that the focus on technology alone would not help to make ships and their operations safer. In order to emphasize the need to address human factors in the design and operation of vessels, the International Maritime Organization (IMO) introduced the term Human Element and encouraged the development of a systemic approach to decrease human and organisational error within the maritime domain. Despite these efforts, rulemaking processes in IMO and the development of maritime safety standards in particular have remained accident driven, and thus primarily reactive.

This article attempts to discuss if resilience engineering can contribute to maritime safety standards becoming more proactive in contrast to being an *"after-the-fact ad-hoc reaction to a single accident"* (Psaraftis, 2002). We will briefly introduce the concept of resilience engineering, safety-I and safety-II and then discuss these concepts within the context of the maritime domain by providing examples for how efforts to improve maritime safety tend to follow the more traditional safety-I (Hollnagel, 2014) perspective. Furthermore, the potential of safety-II (Hollnagel, 2014) and where it might be an asset to the approaches practiced today will be discussed. In the end, some recommendations are given how a resilience engineering perspective can contribute in regulatory developments for safer maritime operations.

2 RESILIENCE, SAFETY-I and SAFETY-II

Resilience as a concept was introduced in the early 1970s and was originally defined as an ecological system's ability to arrive at an equilibrium, or stable state, over time in a dynamic and changing environment (Holling, 1973). In the context of STSs (human operators, technology and organisational settings), resilience is the ability to sustain required operations and achieve system goals under a large variety conditions, including anticipated and unanticipated events. Within the framework of resilience engineering, four cornerstones (monitor,

respond, anticipate, and learn) are used to characterise and analyse system performance in the light of normal operations and disturbances. The focus is on the adaption of performance to the current operating conditions,

with an emphasis on positive examples (Hollnagel, 2006), i.e. situations where the system successfully manages to meet production goals through adapted performance. Another line of research developing from resilience engineering with practical implications, are the concepts of safety-I and safety-II (Hollnagel, 2014). These two concepts represent different approaches to safety management in high hazardous industries. They represent complementary perspectives on how to define, measure, monitor and improve system safety in these industries. Safety-I is often associated with a traditional approach to safety based on quantitative risk assessment, while safety-II is associated with the theoretical concept of resilience and qualitative inquiries into how safety can be identified as the result of successful performance (Hollnagel 2014). Table 1 offers an overview of the salient features.

Within the maritime domain, the research conducted with focus on resilience, safety-I and safety-II is, to the best of our knowledge, sparse and foremost limited to research concerning frontline operations and safety construction in everyday operations (Praetorius and Hollnagel, 2014; Praetorius and Lundh, 2013), as well as addressing using resilience engineering to offer alternative explanations of the concept of human error (Lützhöft, Sherwood-Jones, Earthy, & Bergquist, 2006). Further, the methodological approaches range from simulator studies (Morel & Chauvin, 2006; Bergström et al, 2009) to qualitative inquiry as a basis for functional modelling (Praetorius, Hollnagel and Dahlman, 2015; van Westrenen, 2014).

Table 1: Salient features of safety-I and safety-II (adopted from Hollnagel, 2014)

Definition	Safety arises when the risk of adverse events isas low as reasonably possible	Safety arises when as many things as possible go right.
Safety management approach	Reactive response; safety is improved through eliminating the causes for failures/errors based on examples of what goes wrong	Proactive, trying to identify and anticipate developments and events with focus on what goes right.
	Work-as-imagined as baseline	Work as done as baseline
	Linear and linear complex accident models	Work-as-done as baseline Systemic accident models
Attitudes towards human operators	Humans are sources of error and therefore a liability or hazard	Humans are sources of error and therefore a liability or hazard
Performance variability	Harmful and should be eliminated or decreased as much as possible	Source of flexibility and should be monitored and managed rather than eliminated

3 MARITIME SAFETY STANDARDS IN THE SAFETY-I WORLD

As highlighted before, maritime safety standards have often been introduced in response to accidents (Schröder-Hinrichs et al., 2013) as the question of how an accident can be avoided is a central to all discussions regarding maritime safety. A prominent tool in the IMO rule-making processes is Formal Safety Assessment (FSA) (IMO, 2007). The purpose of this tool is to assist in the identification of safety problems and appropriate countermeasures. Based on quantitative approaches to risk assessment, such as Fault-Tree-Analysis, potential risk reducing measures are evaluated and suggested. Step 1 of the FSA guidelines is consumed with the identification of hazards that may lead to accidents.

However, accidents in the past have demonstrated that STS in the maritime industry have become too complex to be understood by the means of linear or complex linear accident models, which often build the core for traditional risk assessments. The different interactions between operators and subsystems are so diverse and context-dependent that it becomes impossible to forecast a system's performance in its entirety. The work done in a system is often different from the work as it was imagined by the system designers (Hollnagel, 2012). This applies specifically to accident situations. In the aftermath of an accident, safety

improvements and policy making mainly focus on engineering and design solutions (Psaraftis, 2002) in order to "out-design" the possible failure sources.

In complex systems it is, however, very difficult to foresee how even small changes may affect the overall system performance. As a result, we see on the one hand more and more comprehensive safety standards and on the other hand new accident patterns emerging. It is like in the old German tale from the rabbit who challenged the hedgehog for a running competition. The rabbit over-confident of its running skills did not realize that the hedgehog had asked another hedgehog for help. One hedgehog hides soon after the start and the other one waits already at the finishing line and claims that it has already arrived. No matter how many times the rabbit asks to race again, it does not discover the trick and loses the race again. Concentration on one single parameter in a system does not always help to master the overall performance of the system. In a similar way, one could argue that a system adapts to every change so quickly and often in a very unpredictable way that the anticipated increase of safety is not always achieved. The following two examples may highlight this more specifically.

Example 1: Introduction of new enhanced technologies

The introduction of the radar technology in the merchant fleet after World War II has not only reduced the challenges for navigation officers on ships in areas of restricted visibility. It has also caused a new accident category called "radar assisted collisions" as an unanticipated side-effect (Schröder-Hinrichs et al. 2012). Navigators did not reduce the speed any longer in such situations, manoeuvred closer to other ships and thus reduced the safety margin provided by the new radar technology. Similar developments were seen during the introduction of ECDIS and AIS, causing accidents due to over-reliance on technology, poor lookout and improper situation assessment.

Example 2: Fatigue reduction measures

Fatigue has been recognised as a danger for the safe operation of ships and a minimum of 77 hours of rest during a 7-day period with no less than 10 hours a day has been set as an requirement in the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) (IMO, 2011 - refer in particular to Section A-VIII/1 Fitness for duty). It aims to eliminate fatigue as a cause of accidents and errors related to the (cognitive) performance of the seafarers. As a control measure for fatigue management, it is required to keep a record of seafarers' rest hours. While this might be an effective way to address the single cause for an accident (fatigue), it neglects the consequences of this control measure to the organisation and work routines on board. Increased workloads as a result of administrative tasks are a source of complaints from ship officers and engineers, and may also lead to accidents.

The question need to be asked why the focus is to extensively laid on accidents – in other words on things that can go wrong. There are a number of arguments that can be used against this perspective. First, in the maritime business, an accident is still a rare event. Every day, the vast majority of officers and engineers master the challenges related to operations on board ships without causing an accident. Second, a safety-I perspective is characterised by a so-called causality credo impacting the basic assumptions about safety and accidents; i.e. accidents are caused by one or more errors or failures which can be eliminated or neutralised once they have been identified (Hollnagel, 2014). However, human beings are limited in their capability to predict in which ways accidents can be caused in complex systems. Pro-active, probabilistic risk assessment is therefore to a certain extent speculative in its attempts to identify all possible combinations of future courses and events.

One important limitation of the safety-I perspective seems to be its focus on one specific error that occur under very specific conditions of a dynamic STS. If things are mostly go right then the safety-I focus obviously neglects/ignores the ability of a STS to compensate lacks and shortcomings during most of the cases. So, instead of focussing only on accidents, why not to focus on the ability of a system and the ability especially of the operators/actors in the system to do things right and strengthen this capability? Is technology that flexible that it is able to compensate an operator's lack or shortcoming as it is vice versa that the human operator is able to compensate malfunctioning of technical systems?

4 DEVELOPING A SAFETY-II PERSPECTIVE FOR THE MARITIME WORLD

As outlined above, many of the safety-related efforts within the maritime domain focus on improving safety in accordance with a safety-I perspective. This section will therefore in contrast discuss how resilience engineering may contribute to a paradigm shift towards a safety-II perspective in the maritime domain.

Following the capsizing of the Herald of Free Enterprise in 1987, the International Safety Management (ISM) Code (IMO, 2014) was introduced to the shipping industry. The main task of the Code is to clarify the role and the influence of shore-based and ship-based issues/factors in shipboard operations. This was probably one of the few accidents that has led to a systematic review of the STS 'ship' from a holistic perspective. The Code itself consists of two Parts – A and B, whereas Part A deals with the implementation and Part B with the certification of the safety management system to be developed for an individual shipping company. The elements in Part A provide for principles and objectives in a very general way. Unlike most of the IMO standards, the ISM Code is very general for the specific reason that any two shipping companies are different from each other and therefore need different ISM systems. Therefore, a shipping company is free to develop its own interpretation of the requirements under the Code.

The Code contains a few statements that can be used as an argument for the introduction of a safety-II perspective. Companies are required to provide for safe operational practices (Code, paragraph 1.2.2.1) and develop related policies (Code, paragraph 1.4.1). A designated person (DP) responsible for the implementation of the safety management system (SMS) has to be appointed with direct access to the highest management level (paragraph 4). It is furthermore stated that the ISM Code has a self-regulatory nature (MSC-MEPC.7/Circ. 8, paragraph 3.2 – refer to IMO, 2014). However, the ISM Code is deeply rooted in safety-I paradigms. Companies are required to proceduralise the main functions and operations and thus directly pushed in a 'work as imagined' perspective. In the IMO context where a stronger focus is laid on the global eradication of sub-standard shipping this is an understandable objective. Certification guidelines for administrations require objective evidence (A 28/Res. 1071, paragraphs 3.3.4 and 4.12.3 - refer to IMO, 2014), which typically is written procedures, documents etc. This cannot be avoided, but limits the flexibility of a company. The IMO recognizes that prescriptive criteria used by administrations for the verification of the implementation of the Code are counterproductive (A 28/Res. 1071, paragraph 3.1.3 - refer to IMO, 2014).

The ISM Code achievements are discussed controversially. There is no doubt that this tool is a major achievement in the objectives of the IMO to foster a safety culture in the shipping industry. On the other hand, a number of authors (refer, e.g., to Bhattacharya, 2009) claim that it has not developed its full potential. One argument for such conclusions may be that the shipping sector is caught in a compliance culture rather than a safety culture (Mathiesen, 1994). It could also be that the organizational set-up of shipping operations with crews typically supplied by external crewing agencies limits the development of a company based safety culture. This also explains, why the Oil Companies International Marine Forum (OCIMF) considers compliance with the ISM Code only as level one out of four in achieving safe maritime operations (OCIMF, 2008).The safety system of OCIMF specifies various key performance indicators (KPIs) that can be used in order to determine on which safety level a company works. This is a similar development as the Shipping KPIs developed by InterManager. While these indicators are helpful, they just are a mere indication of what has happened in the past (e.g. accident ratios). If a safety-II perspective is to be introduced, a different type of indicators would be needed.

If resilience can be defined as the ability of the system to adjust its performance prior, during and after an unexpected event, a system must have the ability of being proactive. In a wider context, proactivity may indicate an early stage identification of problems or factors that may affect safety together with the development of regulatory actions before an accident occurs. As pointed out above, even though a broad definition may fit and stimulate the scientific discussion, companies and policy makers require measurable indicators to detect and then satisfactorily respond to safety threats. Hopkins (2009) fostered a debate within the (safety) scientific community about the definition of leading and lagging variables. In several scientific contributions the lead/lag dissimilarity, in fact, is strictly related to the distinction between proactive and reactive monitoring of the system. Currently, indicators used by the maritime industry mainly refer to what has occurred in the past (e.g. lagging indicators such as incident/accident ratio, deficiencies/inspections ratio etc.) and are used as potential company performance indicators. Distancing ourselves from the current discussion on a harmonised definition of process and personal indicators, the development of appropriate leading

indicators and their implementation in the SMS, would allow management and regulators to be proactive in managing the causes of accidents (Wreathall, 2009) and work as input to comprehend safety issues from within. Two examples should be given.

Example 1: Anticipating consequences of change

One promising approach to integrate resilience engineering principles in the maritime domain has been suggested by Rigaud et al. (2012). They focus on the problem-solving aspect of FSA (IMO, 2007) that does not take the effects of risk control options into account. Consequently an assessment methodology is suggested based on a mixed-method approach using focus groups, expert interviews and simulation-based exercises to determine the possible side-effects of changes to the overall system performance. Today's complex STSs require the involvement of both frontline operators, company representatives and administrations to make sure that potentially negative side-effects, as well as opportunities for successful operations, are identified and assessed prior to changes being implemented, regardless whether these are technical, organisational or regulatory.

Example 2: Integrating the end-user perspective into system design

Another example might be the currently ongoing CyClaDes project (http://www.cyclades-project.eu). This project aims at developing a framework for obtaining user feedback for the design of shipboard equipment. A benchmarking approach is used for determining how "user-friendly" equipment is designed. This could be used for a proactive assessment of ship safety.

Admittedly, the numbers of examples given here is not very high. There are unfortunately not too many examples at this point in time. The few references are therefore given in order to outline in which direction future research and discussions should proceed.

5 CONCLUSIONS

As discussed above, efforts to increase maritime safety often focus on a reactive approach implementing changes to the system in the aftermath of an adverse event. Further, a large body of research (e.g. Chauvin, 2011; Schröder-Hinrichs et al., 2013) indicates that the maritime domain continues to reflect a safety-I perspective (Hollnagel, 2014) emphasising the need to eliminate the causes of vulnerabilities. While safety-I has been a fruitful approach during periods when systems were tractable and their components had limited interaction, contemporary systems are becoming far too complex to identify and eliminate individual causes. A failure to acknowledge this implies a gap in the stakeholders' understanding of the system and of how it actually operates. Design is always based on assumptions, but as socio-technical systems develop in interaction with their environment, design assumptions must be checked and frequently evaluated. Eliminating the reasons for failure does not help to understand how systems adapt to continue operating in a changing environment.

Although the IMO acknowledges the need to address the human element, there is still a gap in terms of guidance in how to approach this multifaceted issue in a systemic way. Furthermore, as many researchers (e.g. Amalberti, 2001; Dekker, 2011; Vicente, 2006) have stressed, contemporary STSs are too complex to be understood in terms of a structural account of the system and its components. STSs change constantly in response to the demands of their environments. Acknowledging the maritime domain as a complex STS demands not only a new focus on the human element but also the realisation that a new or extended approach to maritime safety and safety management is needed. This does not imply that the current regulations need to be demolished, but that they need to be re-evaluated. At the same time, it has to be realized that the safety-I approach cannot be completely abandoned. Technical specifications in the design of a ship very often need prescriptive regulations. The same applies to the ISM Code, which has to be seen in a wider/global perspective. Nevertheless, the ISM Code is the key instrument to introduce a safety-II perspective in the maritime domain. The safety-II perspective could be seen as a complementary set of principles that could help to achieve and maintain maritime safety. As it was highlighted above, proactive indicators may help to foster the safety-II perspective and more research need to be done in order to expand on the few existing approaches.

Acknowledgement

This paper is a contribution to the project CYCLADES (Crew-Centered Design and Operations of Ships and Ship Systems), funded partially by the European Commission, through the contract nº FP7-SST-2012-RTD-1 313972.

REFERENCES

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science, 37*, 109-126.

Bergström, J., Dahlström, N., Van-Winsen, R., Lützhöft, M., Nyce, J., & Dekker, S. (2009). Rule and role retreat: an empirical study of procedures and resilience. *Journal of Maritime Research, 6*(3), 41-58.

Bhattacharya, S. (2009). *The Impact of the ISM Code on the Management of Occupational Health and Safety in the Maritime Industry*. Unpublished PhD thesis. Cardiff: School of Social Sciences, University of Cardiff.

Chauvin, C. (2011). Human Factors and Maritime Safety. *The Journal of Navigation* (64), 625-632.

Dekker, S. (2011). *Drift into Failure. From Hunting Broken Components to Complex Systems.* Surrey: Ashgate Publishing Limited.

Hollnagel, E. (2011). Prologue: The scope of resilience engineering. In E. Hollnagel, J. Paries, D. D. Woods, & J.

Wreathall (Eds.), *Resilience engineering in practice*. Farnham: Ashgate.

Hollnagel, E. (2012). Resilience engineering and the systemic view of safety at work: Why work-as-done is not the same as work-as-imagined. In Gesellschaft für Arbeitswissenschaft (Ed.), *Gestaltung nachhaltiger Arbeitssysteme* (pp. 19 – 24). Dortmund: GfA-Press.

Hollnagel, E. (2014). *Safety-I and Safety-II: The Past and Future of Safety Management*. Surrey: Ashgate Publishing, Limited.

Hopkins, A. (2009). Thinking About Process Safety Indicators. *Safety Science*, 47(4), 460–465.

International Maritime Organization (IMO) (2007). *Consolidated text of the Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process (MSC/Circ.1023−MEPC/Circ.392)*. IMO Document MSC 83/INF. 2. London: IMO.

IMO (2011). *International Convention on Standards of Training, Certification and Watchkeeping for Seafarers,1978 (STCW 1978) (2011 Edition)*. London: IMO

IMO (2014). *International Safety Management Code (ISM Code) with guidelines for its implementation (2014 Edition).* London: IMO.

Lützhöft, M., Sherwood-Jones, B., Earthy, J. V., & Bergquist, C. (2006). Making safety by tying the knot:

Examining resilience in shipping. Paper presented at the 2nd Resilience Engineering International Symposium, Sophia Antipolis, France, 8-10 November 2006

Mathiesen, T.-C. (1994) Safety in shipping—an investment in competitiveness. In BIMCO (Ed.), *BIMCO Review 1994* (pp. 56-58). Copenhagen: BIMCO.

Morel, G., & Chauvin, C. (2006). A socio-technical approach of risk management applied to collisions involving fishing vessels. *Safety Science, 44*(7), 599-619.

Oil Companies International Marine Forum (OCIMF) (2008). *Tanker Management and Self Assessment 2*. Bermuda: OCIMF.

Praetorius, G., & Hollnagel, E. (2014). Control and resilience within the maritime traffic management domain. *Journal of Cognitive Engineering and Decision Making, 8*(4), 303-317.

Praetorius, G., Hollnagel, E., & Dahlman, J. (2015). Modelling Vessel Traffic Service to understand resilience in

Everyday operations.*ReliabilityEngineering & SystemSafety*(inpress).doi: http://dx.doi.org/10.1016/j.ress.2015.03.020

Praetorius, G., & Lundh, M. (2013). "Under dangerous conditions" - safety construction and safety related work onboard of merchant vessels. Paper presented at the 5th Resilience Engineering International Symposium, Soesterberg, The Netherlands, 25-27 June 2013.

Psaraftis, H. N. (2002). Maritime safety: To be or not to be proactive. *WMU Journal of Maritime Affairs*, 1(1), 3–16.

Rigaud, E., Lützhöft, M., Kircher, A., Schröder-Hinrichs, J.-U., Baldauf, M., Jenvald, J., & Porathe, T. (2012). Impact: More Than Maritime Risk Assessment. *Procedia - Social and* Behavioral Sciences, 48(0), 1848-1854.

Schröder-Hinrichs, J.-U., Hollnagel, E., & Baldauf, E. (2012). From Titanic to Costa Concordia – a century of lessons not learnt. *WMU Journal of Maritime Affairs*, 11(2), 151-167.

Schröder-Hinrichs, J.-U., Hollnagel, E., Baldauf, M., Hofmann, S., & Kataria, A. (2013). Maritime human factors and IMO policy. *Maritime Policy & Management*, 40(3), 243–260.

Vicente, K.J. (2006). *The Human Factor.* New York: Taylor & Francis Group.

van Westrenen, F. (2014). Modelling arrival control in a vessel traffic management system. *Cognition, Technology & Work, 16*(4), 501-508.

Wreathall, J. (2009). Leading? Lagging? Whatever! *Safety Science*, 47(4), 493–494.

RULE 'VIOLATIONS' AND RESILIENCE IN HEALTHCARE

Jonathan Back[1], Janet Anderson[1], Myanna Duncan[1] and Alastair Ross[2]
[1] Centre for Applied Resilience in Healthcare, King's College London, UK. [jonathan.back; janet.anderson; myanna.duncan]@kcl.ac.uk
[2] University of Glasgow, UK.
[2] alastair.ross@glasgow.ac.uk http://resiliencecentre.org.uk/

Abstract

There are many explanations for the violation of rules, and in this paper we report on examples from a healthcare setting. The research explores how nurses conceptualise safety rules when using medical equipment to treat patients. Do nurses intentionally violate the formalised rules set by the hospital and regulatory authorities? Unlike other work on rule violation, the focus here is on understanding how rule violation can be used as a measure of necessary performance variability. We found that the nurses studied had a limited awareness of what rules they were adhering to or intentionally violating. Instead, nurses performed the work in a way that was consistent with their own understanding of safe practice. Informal and dynamic safety behaviours were central to how resilience was created and sustained. Better management is needed to avoid situations where well-intentioned violations are not shared amongst colleagues. This is because a lack of team awareness can result in conflicting safety goals and potentially unsafe practice. When informal safety behaviours are shared, risks are open to group inspection.

1 INTRODUCTION

The conventional view on risk management considers human performance variability, of any kind, as a threat to safety and something that should be avoided. However in the Resilience Engineering community, it is asserted that performance variability is necessary and useful (e.g., Woods, 2006; Dekker, 2003). This is because in complex adaptive systems, work cannot be completely specified in advance. Indeed, safety rules often have to be violated when responding to threats and disturbance (*see* Hale & Borys, 2013). Woolfson et al. (1997) argued that rule violations could be evidence that workers are 'involved in the process of risk assessment as fully legitimate active participants'.

There are many explanations for the violation of rules, and in this paper we report on healthcare examples by using a framework developed by Reason (1990). This framework was originally developed to account for human error. Violation can imply deviance and intentional harm. However from a human error perspective, violations can also occur when they are well-intentioned, targeting desired outcomes such as patient safety. In this paper the focus is on well-intentioned violations.

According to Reason (1990) explanations for the violation of rules include:

- **Routine violations** that have become a normal and accepted way of behaving.
- **Situational violations** in response to specific situations where the rules are not relevant.
- **Exceptional violations** in response to situations never before encountered; and optimising adaptations, done to explore the boundaries of system operation.

This paper aims to discover if these types of violations can be studied in healthcare practice. Unlike other work on rule violation (*see* Hale & Borys, 2013), the focus here is on understanding if rule violations can be used as a measure of performance variability. It has been suggested that 'outcomes emerge from human performance variability, which is the source of both acceptable and adverse outcomes' (Hollnagel, Wears & Braithwaite, 2015). Hospital managers and clinicians 'understand' what human error is. Conceptualising what is meant by performance variability is much harder. This paper attempts to make this conceptualisation easier.

2 BACKGROUND

In the UK patient care is becoming increasingly complex with a mixture of chronic and acute conditions to be managed, and a tangle of new and old care pathways. There is also a constant state of technological change, e.g., paperless records and e-prescribing. These factors, along with the under-resourcing of the National Health Service (NHS), mean that the demands on healthcare providers are rarely predictable. The good news is that in most cases the NHS works, and patients get treated effectively. One reason for this could be that the organisation has the

inherent capacity for resilience, i.e., clinicians often have to work around problems, devising solutions and making things work for patients despite pressures. However, it remains a source of frustration that progress on patient safety is patchy, and that patients are being harmed every day by errors that are avoidable (Leistikow et al., 2011).

Allowing clinicians to engineer multiple paths to successful patient care is ostensibly in conflict with promoting a standard rule-based way of working. In this paper this conflict is examined by studying the task of setting up an infusion device, which is an exemplar of an everyday nursing task. Infusion devices are widely used in hospitals, and allow for treatment (medication) to be given to a patient over a period of time at a predetermined rate.

Within the UK there is a range of rules and standards on how to setup an infusion device. These have evolved over time in response to clinical incidents, rather than to the changing demands of work practice. For example, infusion devices are now used to deliver a range of treatments that were previously administered in a different way. During nurse training the Standards for Infusion Therapy by the Royal College of Nursing are typically followed (RCN, 2010). When working in a hospital there are Hospital Trust rules that need to be adhered to. In addition, each clinical area within a hospital will often have supplementary standards and guidelines. All these need to be considered alongside the instructions provided by device manufacturers, which are specific to the models of devices being used. Our study explores the extent to which these rules and standards are adhered to.

Before reporting the study, we reflect on the ideology of standard work in healthcare:

> "We know we need standard work in order to avoid the chaos of many people performing the same process in different ways, which creates variation and the need for workarounds" (Barnas, 2014).

It has been claimed that the standardisation of work can result in a demonstrable reduction of errors across some processes within some hospitals. For example, in Thedacare Hospitals (USA), a new standard led to the near elimination of medication reconciliation errors in inpatient units (Barnas, 2014). The need for this new standard was discovered by applying Lean management principals, which aim to better understand problems by performing root cause analyses in situ. Lean principles are derived from the Japanese manufacturing industry (Krafcik 1988). They are predominately about the identification and steady elimination of waste by promoting standard rule-based ways of working. If errors can be nearly eliminated by designing a new standard way of working why is resilience needed?

There are tensions between the need for standardisation versus the need for adaptability. It is suggested that people have learned to adjust what they do to match actual work conditions, resources and constraints (*see* Hollnagel et al., 2006). It is thought that the complexity and unpredictability of a healthcare work environment requires people to develop the adaptive capacity to handle everyday work (e.g., Hollnagel, Wears & Braithwaite, 2015). Within healthcare, there are heroes (at all levels and roles) that keep the system functioning (Barnas, 2014), by responding to new pressures. Indeed, it is also argued that there is too much reliance on resilience (Wears & Vincent, 2013). This paper explores the difficulties in balancing the need for standards and rules, and the need for resilience when using infusion pumps, and considers implications for safety from an organisational perspective. We explore these notions by considering concrete examples.

3 METHOD

3.1 Participants

The director of nursing, at one large NHS hospital in the UK, provided the names of nursing ward managers in clinical areas where infusion pump use was prevalent. Eight areas were contacted and a positive response was received from six. Each of these ward managers were asked to recruit five nurses who would be appropriate for the study. Our inclusion criteria were that they should be qualified staff nurses, who have undergone training with the infusion pump device, and that they regularly administer intravenous therapy. In total, n= 14 nurses across five clinical areas completed the study.

3.2 Research Design

There were three phases to the study. The first phase was a semi-structured interview where details about a participant's experience relating to the administration of intravenous therapy were elicited. The second phase involved a participant collecting and redacting photocopies of prescriptions that they had recently

administered using a pump. The third phase was an observed simulation where a participant demonstrated the programming of an infusion pump using the example prescriptions that they had collected.

3.3 Procedure

Initial interview. Written consent was obtained before the interview began, and permission to make an audio recording was also sought. After the thirty minute interview was finished, the participant was briefed on the second phase of the study.

Prescription data collection. Over a period of one week the participant was required to collect and redact photocopies of prescriptions. The participant was then scheduled to attend a simulation session, one to two weeks after the initial interview, to talk about the documentation they had collected.

Observed simulation (cognitive walkthrough). The session lasted one hour. The participant was asked to select two different examples of therapies that had been recently prescribed, and that they had collected documentation on. For these two therapies the participant was asked to describe the steps they performed in detail, and demonstrate the programming procedure on a training pump. The programming procedure was captured on video. Only a participant's hands / arms were visible, and written consent was obtained. After each demonstration, a debriefing interview was conducted. This probed the differences between what was demonstrated versus actual practice on the ward. By demonstrating and then reflecting on practice, it was hoped that a detailed account of different work patterns would be obtained.

The same model of infusion pump is used across the hospital, although some clinical areas have different functionality enabled such as a drug library in the Intensive Care Unit, and the ability to adjust the pump pressure in Paediatrics. However, the basic programming task was the same across all of the pumps. This involved entering the VTBI value first, as mandated by the device, and then choosing to enter either the RATE or TIME value. The prescription chart / sheet and other documentation used during the programming procedure varied between the different clinical areas, as did the types of therapies administered.

3.4 Analysis

For the purposes of this paper, the violation framework developed by Reason (1990) was used to categorise instances where participants varied from standard procedure. During the interviews and simulation, participants were asked to describe what the standard procedure was. The hospital guidelines for performing infusions using a pump were cross-referenced to check for incongruities. Selected situations were abstracted into scenarios enabling a description of a work practice pattern.

4 RESULTS

During the first interview phase all participants suggested that using an infusion pump (as part of their current work practice) was straightforward. Overall the nurses were satisfied with the training that they received on the pump from the device manufacturer. They also talked positively about attending mandatory update sessions that outlined Hospital Trust standards and rules. When asked about what was most difficult, the focus was on correctly preparing the drug in the bag prior to using the infusion pump. The entry of values into a pump was not considered to be an especially important task step or particularly problematic. When nurses were asked where these values originated from, most said that they were already familiar with them, or that they simply retrieve values from the drug label or patient's prescription chart.

The second session with participants involved asking them to demonstrate how pumps are programmed. Based on the interview data in the first session, it was expected that there would be little variance in how pumps are used. However as was discovered, nurses 'violated' rules on an everyday basis for a variety of different reasons. After each demonstration, participants reflected on how the pump was 'actually' programmed on the ward. This revealed twenty examples of violations / adaptations. Many of the nurses admitted that they had not had the opportunity to talk about the intricacies of their work before. Although the session was scheduled for one hour, some participants were enthused and sessions frequently overran.

4.1 Routine violations / adaptations

Findings challenge the assumption that the procedure of using an infusion pump is an activity that is executed by following formalised rules set by the hospital. Routine violations were performed because nurses had to adjust and adapt their performance in response to the way the team on the hospital ward operates. As demonstrated

in the examples described below, nurses have their own personal conceptualisations of safe practice. Not sharing these can result in misguided safety goals.

Routine Violation Example 1. Nurses with over five years of experience of using different models of infusion pumps, unsurprisingly had a conceptualisation of safe practice that was different to nurses who had only ever used the latest infusion pump model. These more experienced nurses were familiar with calculating dosages from first principles, which meant that they were happy to recalculate doses themselves. In one scenario, nurses who regularly work together administering chemotherapy made a routine adaptation to their practice so that clinic appointment times were less likely to overrun (a threat to patient safety and experience). For example, when a doctor prescribes a chemotherapy treatment to be administered to a patient over three hours, the electronic prescribing system would calculate the required rate of the infusion. The less experienced nurses would simply transcribe this rate into the device. However, because the process of starting and stopping the pump at various stages of administration takes time (e.g., when flushing bags and priming lines), the therapy would actually be delivered over a longer time than prescribed. More experienced nurses now work with the less experienced nurses, adjusting the calculated rate of infusion so that the therapy is delivered on time and the clinic does not overrun. In this case nurses are violating procedure by not entering the infusion rate value shown on the electronic prescribing system.

Routine Violation Example 2. Two of the nurses interviewed believed that they should always enter an infusion volume that was less than the prescribed amount. The rationale for doing so was that they did not want the drug bag to run dry (empty), which would harm the patient as air would be infused instead. However, the infusion pump is designed to stop any air (including small bubbles) from being infused. Adjusting the prescribed value is unnecessary, and makes monitoring how much therapy was intended to be delivered harder (especially problematic when a different team member takes over care). Another nurse suggested that she enters an extra 10ml when programing the pump because of bag overfill by the drug manufacturers. However drugs prepared by pharmacy are not overfilled, so this adjustment is unnecessary. These routine violations are based on misunderstandings. It was suggested by one of the matrons that we interviewed that nurses are always personally responsible for the pumps that they program, and individual approaches are rarely discussed unless there is a noticeable impact on the team's performance.

4.2 Situational violations / adaptations

Do nurses intentionally violate the formalised rules set by the hospital and regulatory authorities? We found that the nurses studied had a limited awareness of what rules they were adhering to or intentionally violating. Instead, nurses performed the work in a way that allowed for the development of informal and dynamic behaviours with patient-safety or patient-experience in mind. As described in the examples below, the use of these informal safety behaviours can fluctuate on a daily basis. This is dependent on the skill mix of the staff on a particular shift and the types of patients being treated.

Situational Violation Example 1. In Paediatrics it is important that nutrients delivered using an infusion pump are recorded every 24 hours. To facilitate keeping track of how much therapy a patient has received, two nurses in Paediatrics reported that they reprogrammed pumps at midnight, which resets the pump's volume infused counter. This workaround made it easy for nurses during the day to check (at a glance) how much nutrients a patient had received in a 24-hour period. A third Paediatrics nurse (who worked in the same team) suggested that re-programming at midnight is not always sensible because staffing levels are lower and sometimes less skilled, and patients might be unnecessarily disturbed.

Situational Violation Example 2. In an outpatient clinic setting using an infusion pump to deliver blood products can sometimes take over four hours. This can be frustrating for patients who need to return home or to work. One nurse reported that she sometimes increases the infusion rate so that patients can leave faster. This involves careful monitoring of the patient, and is a patient-safety versus patient-experience trade-off.

4.3 Exceptional violations / adaptations

Conceptualising what is meant by performance variability is not possible without appreciating that it is the intrinsic variability in everyday work that allows for resilience to threats. In the examples of exceptional violations presented below, both individuals and teams are able to adjust and adapt their performance.

Exceptional Violation Example 1. Some new trial therapies require scaled doses, starting small and rising incrementally. These treatments have protocols associated with them. However protocol documents are often poorly designed with unnecessary information, and are sometimes difficult to interpret. In one scenario, a nurse identified that the new trial documentation was potentially confusing, and redesigned the document to avoid the potential for error. This document was appropriated by other nurses, and worked well with no adverse outcomes reported. It transpired that the treatment in question was frequently erroneously administered at other hospitals. Nurses were aware of the need to anticipate problems and to ensure that additional resources were available in case they were needed (in this case the unofficial protocol document).

Exceptional Violation Example 2. On a ward an unusually large number of patients were receiving infusion therapy and staffing levels were below normal. This meant that patient infusions would finish and there would be a delay in the continuation of therapy (changing over drug bags). Nurses on the ward developed a strategy and programmed the pump so that it would alarm early, notifying nurses that the new drug bag should be prepared. This worked well until there was a shift change. Incoming nurses could not calculate how much therapy a patient had received because the pumps were programmed in a non-standard way.

5 DISCUSSION

The examples highlighted in this paper demonstrate the complexity and unpredictability of a healthcare work environment, and the requirement for individuals and teams to make adaptations and adjustments to everyday work. There is no standard way of working even when using equipment that is standardised throughout the hospital (all the clinical areas have the same make and model of infusion pump). The results from this study of a seemingly bounded task show that understanding performance variability is possible, but classifying adaptive behaviour by suggesting they are well-intentioned rule violations (Reason, 1990) might be naïve.

We found that the nurses studied had a limited awareness of what rules they were adhering to or intentionally violating. Instead, nurses performed the work in a way that was consistent with their own understanding of safe practice. This involved adjustments and adaptations to work in response to:

- Accepted ways of behaving within their peer group.
- Specific situations where the standard rule-based approach was not relevant.
- Making trade-offs to maximise levels of patient safety and patient experience.

Nurses do not behave algorithmically; instead they recognise cases from previous experience and adapt. This is a source of resilience. Nurses were aware of the need to anticipate problems and to ensure that resources were available in case they were needed. This awareness impacts on performance even when planning routine tasks. Nursing behaviour was not constrained by formalised rules when using infusion pumps. Instead they devised their own working practices with an implicit and sometimes wrong model of safe behaviour. Studying these working practices, and then comparing them across other clinical team members, allows us to consider which may increase the likelihood of desirable outcomes.

The informal safety behaviours identified appear to enhance the capacity of the system for resilience. Many are socially distributed and managed across the clinical team. Despite the existence of shared informal behaviours, it was also found that individuals had their own conceptualisations of safe practice. Some of these personal conceptualisations involved risky and potentially unsafe workarounds. This led to situations where some nurses were performing work tasks and violating formalised rules without thinking about or recognising the risks involved. There is a need to understand these adaptations in more detail, and to better manage the likelihood that they lead to desirable outcomes.

In the study of infusion pump use reported in this paper, it is difficult to conceive how the development of new rules and standards could replace the need for adaptive performance as suggested by Barnas (2014). Wallace and Ross (2006) argued that “Instead [...] of rules with the hidden implication ‘do this or you will be fired’, they should perhaps be offered more in a ‘these are some of the methods we have developed of doing these particular tasks here, and we have found them useful” p219. Although the task of using an infusion pump appears relatively straightforward, there is significant performance variability between individuals who often have varied, and in some instances conflicting safety goals. When informal safety behaviours are shared, risks are open to group inspection.

6 CONCLUSION

This research aimed to discover if rule violations can be studied to better understand performance variability and the capacity for resilience. Findings provide evidence that formalised rules do not constrain the performance of nurses in a way that discourages adaptive performance. Understanding why rules are violated reveals informal safety behaviours, which are central to how resilience is created and sustained.

Organisations need to better manage adaptive performance within safety-critical work environments. Healthcare practitioners have a personal responsibility for the safety of their patients. Their conceptualisation of safe practice is also personal. Thus, performance variability is intrinsic to healthcare practitioners. Our work provides evidence of situations where formalised rules have been 'violated' and superseded by informal safety behaviours. This may enhance the capacity for organisational resilience, in instances where informal safety behaviours are socially distributed and risks are open to group inspection. Better management is needed to avoid situations where safety behaviours are not shared resulting in conflicting safety goals.

"In (the hospital)…hardly anyone knows all the extant rules, much less exactly which situations they apply to for whom and with what sanctions. If this would not otherwise be so in our hospital it would be true anyway because of the considerable turnover of nursing staff. Also noticeable to us as observers was that some rules once promulgated would fall into disuse, or would periodically receive administrative reiteration after the staff had either ignored these rules or forgotten them" Strauss et al. (1963).

Acknowledgements

We thank the NHS staff who participated in this study. This study was approved by the NHS Trust's R&D Department and was conducted as part of CHI+MED: EP/G059063/1. We would like to thank the Guy's and St Thomas' charity enabling the establishment of the Centre for Applied Resilience in Healthcare.

REFERENCES

Barnas, K. (2014). Beyond Heroes: A Lean Management System for Healthcare. ThedaCare Center for Healthcare Value.

Dekker, S. (2003). Failure to adapt or adaptations that fail: contrasting models on procedures and safety.Applied ergonomics, 34(3), 233-238.

Hale, A. & Borys, D. (2013). Working to rule, or working safely? Part 1: A state of the art review. Safety Science, 55, 207-221.

Hollnagel E., Wears R. L. & Braithwaite J. (2015). From Safety-I to Safety-II: A White Paper. The Resilient Health Care Net: Published simultaneously by the University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia.

Hollnagel, E., Woods, D.D. & Leveson, N., eds. (2006). Resilience engineering: Concepts and precepts, Ashgate, UK.

Krafcik, J. F. (1988). Triumph of the lean production system. Sloan management review, 30(1), 41-51.

Leistikow I. P, Kalkman C. J & de Bruijn, H. (2011). Why patient safety is such a tough nut to crack. BMJ, 342:d3447.

Reason, J. (1990). Human Error. Cambridge University Press, Cambridge.

RCN. (2010). Standards for Infusion Therapy. 3rd Edition, Royal College of Nursing.

Strauss, A., Schatzman, L., Ehrlich, D., Bucher, R. & Sabshin, M. (1963). The hospital and its negotiated order, Macmillan, London.

Wallace, B. & Ross, A. (2006). Beyond Human Error—Taxonomies and Safety Science, CRC Taylor and Francis Group, New York.

Wears, R. L. & Vincent, C. A. (2013). Relying on resilience: too much of a good thing? In E. Hollnagel, J. Braithwaite, R.L. Wears (Eds.), Resilient health care, Ashgate, UK, 135–144.

Woods, D. D. (2006). Essential characteristics of resilience. In Resilience engineering: concepts and precepts, Aldershot: Ashgate: 21-34.

Woolfson, C., Foster J. & Beck, M. (1997). Paying for the piper. Mansell, London, 334-336.

MORE REQUIREMENTS, MORE SAFETY? CHALLENGES IN COMBINING STRINGENT REGULATION WITH RESILIENT DESIGN

Mikael Wahlström, Pia Oedewald, Nadezhda Gotcheva, Kaupo Viitanen
VTT Technical Research Centre of Finland Ltd, Vuorimiehentie 5, FI-02150, Espoo, Finland
mikael.wahlstrom@vtt.fi
www.vtt.fi

Abstract

This paper discusses safety-relevant threats involved in highly regulated design. The study draws from an interview study regarding two design projects, a minor modification and a large waste management system, at two nuclear power plant (NPP) sites in Finland. The cases portray some main elements in NPP design, among which are stringent regulation, time-consuming document drafting, and throrough requirement management. We identify relevant trade-offs related to design of this kind and discuss the possible threats involved. The trade-offs include a rigid model of design and time-consuming document-based communication. The implied (though not empirically demonstrated) threats include insufficient iteration of the design idea, lack of holistic focus on the end-product, sharing the design authority with the regulator, and challenges in creating design solutions that promote resilience through operators' positive contribution to safety. Overall, we suggest that stringent regulation, comprehensive requirement management, and up-to-date reguirements are not sufficient in providing safe designs. Mindfulness of the identified threats, safety culture emphasizing the design organization responsibility, and leadership that ensures system thinking are needed as well.

1 INTRODUCTION

This paper reports on an interview study on design activities in the nuclear domain in Finland. The aim of the study is to identify possible threats, which should be taken into consideration in order to avoid the generation of failed designs. This is important because weaknesses in design have played a part in major accidents in the NPP domain (Rollenhagen, 2010). Our arguments, however, do not merely apply to the NPP context, but various safety-critical domains as well where designing is done 'by the book', and therefore are of interest for a wider audience. By design, in turn, we refer to activities such as idea conception, planning, problem solving, and decision making concerning technical modifications and development of new technological solutions, and the overall management of these activities (e.g., Aspelund, 2006). Based on the interviews, the NPP design practices in Finland seem to entail several positive elements, which are of key value for safety, such as thoroughness, stringent regulation and adherence to the international standards.

One might indeed immediately assume that safe designs can be achieved simply by the means of comprehensive and up-to-date set of requirements and by stringent regulatory overview. However, in order to expand the view and to provide a critical approach, we assume that this is not the whole truth. These elements certainly contribute to the safety of the end-product, but they may also come with some trade-offs and effects that have the potential to be negative for safety as it is understood in resilience engineering perspective (Hollnagel et al., 2011) and in other practical terms. The argument goes that if the design activity entails huge amount of technical requirement management and drafting precise documents for the regulator, a trade-off emerges: either too little effort might be dedicated to iterating the design idea and to considering the design in terms of usage at a system level, or the design process might become extremely time and resource consuming.

We will firstly provide a description of the basic working practises in Finnish NPP design and after that consider some possible drawbacks. We do not criticise the way nuclear projects, new builds or modifications, are actualized in Finland as such, since it seems that requirements and standards are considered with precision by both the regulator agency and the power companies. However, when it comes to the NPP domain especially, one should be open-minded in considering possible sources of incidents and failed designs.

Regarding the research approach, the present study is thus somewhat speculative as it draws from empirical findings in order to identify logically plausible hypotheses on as to why designs could fail rather than directly identifies empirical precedents. In our view, however, this is an acceptable approach in studying high-risk domains: NPPs are built to withstand harsh physical conditions that are unlikely and do not have notable precedents, but which are nevertheless in principle possible; one could imagine the example of a huge earthquake in the stable tectonic plate under Finland – extremely unlikely but something to be prepared for. The same reasoning applies to human error issues and design: one should consider human behaviours, which perhaps have not taken place, but which seem plausible given the actual working conditions. In addition, we will shortly contrast the existing design practices to

the concept of resilience engineering – we discuss that it could be challenging to design in a manner such that supports operators' capability to provide positive contribution to safety in unexpected situations.

2 THE TWO BASIC ELEMENTS IN NPP DESIGN: REGULATION AND DOCUMENTATION

Our study draws from interviews on two design cases, which are explained here only briefly. The method and the cases are explained more comprehensively elsewhere (Wahlström, in press). The first NPP design task could be considered fairly simple: it included a minor modification to a pump functionality and did not require designing new components as changes to circuit diagrams were sufficient. In contrast, the second design case was a major long-term project: the overall design for management of a specific kind of waste and the associated infrastructure. The interviewees were involved in the design work and included eight energy company workers and a governmental regulator representative. In the following we will explicate some of the basic findings based on the interviews regarding the case studies.

The pump functionality modification case, despite being technically a fairly simple task, took 17 months of research and communication before the actual work could be initiated. First, two months of internal decision-making took place within the power company and after that a comprehensive 21 page plan, called 'preliminary plan' was drafted for 10 months. This included a major effort in studying the requirements involved in the modification work. The document drafting took a considerable amount of time from an engineer and also included the circulation of the text in-house within experts from different fields who commented the plan. After that the document was sent to the safety authorities who gave their first response in three months. The governmental regulator representative concluded that the document is not sufficiently comprehensive, as it did not include sufficient details on testing the new design for verifying its functionality. The issue was then addressed and the project was finalized successfully. As seen in this design case, the relation between the power company and the regulator could be described as formal: the decisive communication takes place with detailed documents. They communicate in other ways as well, that is, by telephone, by more casual emails and sometimes face-to-face even, but the final decisions are based on the documents. It seems that this formality has not always been the only way of working in Finland:

'We also have experienced people here, quite a few of them, and they're used to calling the authorities and simply telling them that we've thought about implementing this kind of a system, sounds good, doesn't it? And the authorities say splendid, and they implement it. I mean this is how it was done 10 years ago. But it doesn't work like that anymore, so what happens is, these, how should I put it, old dogs, they'd like to keep doing things the old way, like they used to, without sending this and that and the other thing there. But we do have to do it now.' (Energy company employee, the modification case)

Overall, it seems, in the pump functionality modification case the biggest challenge and effort were the document drafting and communication of the plans with the authorities.

'Let me put it this way, if we were producing dairy products here and not nuclear power, the design would have been pretty much there already, but we have to write a mountain of documents in addition to this. […] If you want a challenge, what's challenging is communicating with the authorities, in writing, on paper you know, since what we do is we may discuss an issue with the authorities over the phone and both parties are aware of the fact that writing unambiguously, it's incredibly difficult. […] And also, in addition to the extra, in addition to the usual circulation, we had three or four internal review cycles at the office, checking everything from spelling to comprehension, so I'd say all of this has made the document clearer, easy to understand.' (Energy company employee, the modification case)

The importance of formal and precise documents is clear throughout the interviews. There was some variation in the connections with the regulator, however, as in the larger waste management project, a dedicated person from the regulator organization was available for the project and could provide feedback more efficiently. Nonetheless, also in that project, requirement management as well as general project management were time-consuming and challenging efforts. In other words, what is very descriptive of the design processes in the nuclear domain is the vast number of requirements that have to be taken into account as the documents are drafted. This could be seen as an evolving phenomenon, as the number of requirements has been on the rise. It was mentioned in particular that after the Fukushima Daiichi disaster in 2011, more and more safety requirements were introduced.

Overall, three distinctive characteristics are descriptive of design in NPP domain in Finland, these being 1) meticulous management of up-to-date set of appropriate requirements, 2) clear documents for transparency and

3) thorough regulatory oversight. Though these phenomena are positive in ensuring that the design solutions are safe, they might entail some counterproductive elements as well.

3 POSSIBLE DRAWBACKS AND THREATS

There are at least two possible conditions, in which the combination of stringent regulation and the plurality and complexity of requirements could be insufficient in providing successful designs. Firstly, one could see these issues as 'trends' that increase hand-in-hand with the line of time, and especially if major incidents occur, such as the one at Fukushima; in view of the interviews, this kind of progression has been taking place. New requirements can be necessary, but at the same time one should consider that, in principle, there must be a limit beyond which the number of requirements produces negative effects: this is because eventually the requirement management and document communication process could become so effortful that the design process becomes too 'rigid' in a practical sense. Secondly, it is notable that human activity is never perfect and at times mistakes occur, especially under stress, such as when working with multiple tasks parallel, or when having to balance with various, partly conflicting goals of the different stakeholders. We will discuss that 'losing the big picture' could be a plausible cause of mistakes in design in extremely regulated and complicated technology domains.

3.1 Lack of flexibility and the effortfulness of iteration

The working practice in NPP design where perfect and comprehensive plans are needed prior to implementation suggests that near perfect foreknowledge on the state of affairs at the plant are needed as well. Given that drafting of these plans takes several months, it implies that the designers have to be able to 'foresee' months or years into the future. They have to have all the details beforehand. Could this then be a problem? One may ask whether the plans could become somehow outdated during the process of their writing and during the waiting for the regulator feedback? Obviously, the plans can be modified during the document drafting if, for example, new requirements are introduced. Nonetheless, it seems that the design concept is quite fixed to the original plan; the design idea as a whole cannot be conveniently changed after the initiation of the document drafting and requirement study.

Thus, the design model applied in NPP design resembles the so-called V-model (Figure 1); it entails the assumption that the foreknowledge is perfect. Turner (2007, p. 12) describes the V-model as follows: 'we can define complete, consistent, testable, and buildable requirements; decompose perfect requirements to perfect specifications; accurately estimate effort, cost, and schedule for the specifications; schedule work according to this information early in the programme; and measure progress using earned-value management or similar techniques'. Indeed, Turner points out that the V-model can be criticised due to the lack of flexibility. This criticism concerns the NPP design as well.

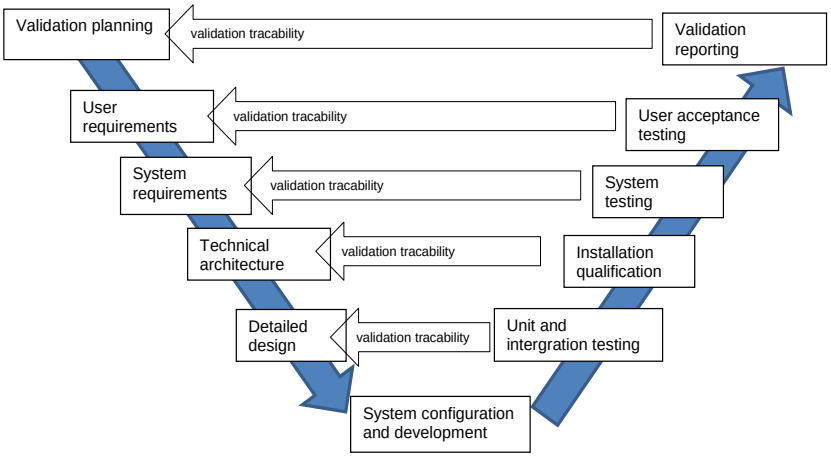


Figure 1. V-Model of a Conventional, Large-System Development Process (adapted from Turner, 2007).

The argument then goes that, once an agreement on the design solution has been made, a long process of requirement management and document drafting takes place – and during this requirement study and drafting phase the plans can be changed only slightly, i.e., it would be a somewhat rigid process. Alternatively, the plans could be changed more drastically but this would imply that the burdensome document drafting and requirement management process should be re-done as well. In other words, two options exist, and both could be seen as problematic: either the process is rigid and non-changeable, or the process is especially time and resource consuming.

Firstly, to address the problems of a rigid and predefined process, one should consider the issues, relevant to a NPP design solution that might vary over time, i.e., the issues that could be different than those foreseen. These unpredictable issues could include, at least requirement changes, changes in design or implementation work force, advances in technology and supplier situation. If the situation changes, while the plans have been laid down already, new plans would be needed. Additionally, parallel design projects might have an impact as well, that is, if several design projects with interlinked causal elements take place at the same time and if all of these projects progress especially slowly, managing the overall repertoire of projects might be particularly challenging.

Secondly, one may accept the fact sometimes new plans have to be made despite the great efforts involved. The safety-related problem involved is easy to identify: if things do not get done in a reasonable time, there will be delays in creating the necessary enhancements to safety. More generally, economic expenses in this approach would be considerable. To the best of our understanding, it is likely that this is actually how things are done in the NPP domain in Finland. According to our interviewees, there are sufficient economic resources to be used when dealing with design issues concerning safety.

Overall, one could conclude that iteration of design plans is effortful in NPP projects. It is thus questionable whether the designers are always when necessary willing to reconsider a design idea, if this reconsideration implies a new burdensome document-drafting and requirement management process. It is very unlikely to find data confirming this kind of behaviour, but one may consider it as a possible phenomenon seeding unsuccessful design solutions in some circumstances. This is threat that might take place in stressful or hurried work conditions.

3.2 Losing the big picture?

Understanding the overall NPP context has been found to be a significant challenge in NPP design (Macchi, et al. 2014). This is understandable in view of technical complexity. Additionally, one may thus assume that with a tremendous amount of document creation and tasks project administration tasks, the possible problem of not understanding the end-product holistically could be amplified: arguably, there could be the possibility that the design team distances itself from the actual aim, that is, the creation of a good solution, since there is so much other issues involved.

In other words, as it takes time in document drafting and requirement management, it might be that these activities become the focus of design work – the actual usage of the final technical solution could remain secondary. This could be seen as a leadership issue: a good leader would maintain an overall understanding and responsibility of the actual solution rather than focus on project and requirements management. The following account exchange concerns initially good cooperation, but then goes beyond that in discussing leadership.

> *Researcher: 'Can you think about any practical way of making sure that there is no break [in cooperation]?'*
>
> *Interviewee: 'Yeah. It's what we have now. [Project leader name], he's in charge of the project. During the implementation of the project, there was no such person. So somebody has to have an interest in what's being done. So that's the basic element that, there's one person who feels that this is mine, on the operator side, who feels that now I'm responsible; my team will operate this plant. Then, the approach is completely different. If nobody's nominated, then who should care what's being done. Nobody. Would we have been, or would we have had such a person during the project, it would have been a bigger success.'* (Energy company employee, the waste management system case).

Understandably, in large and complex projects the leader cannot maintain a specific understanding of all the relevant technical issues. Challenging and important design tasks, that is, those with significant safety and/or economic implications, are typically organized as projects. The projects would thus have to be viewed from a sufficiently broad level of abstraction. The project leadership should maintain an overview of who understands the issues relating to its more specific subdomains. The leader should also make sure that these individuals communicate with each other and the leader should maintain the big picture sufficiently.

Another issue that could possibly induce the lack of maintaining the big picture is shared responsibility. Arguably, the fact that the power companies in Finland rely on the authorities in checking that designs are acceptable, could mean that the power companies, in a sense, share responsibility and 'design authority' with the regulator agency. In a high reliability organization someone should have to have the final word and the responsibility in ensuring that the design solution works – someone has to maintain the 'big picture'. As expressed in an IAEA report (2003), and according to the regulations, the operating organizations, that is, the power companies, have the responsibility to maintain design authority. This is to say that they have to formally approve all the design changes and also have to maintain the needed knowledge. However, the regulator agency in Finland has responsibilities that could be seen as overlapping as it also accepts the plans. In some instances this could imply a loss of design authority in the actual

working practices of power company workers, i.e., the designers could start thinking that 'if the regulator accepts, the design is ok'. Actually the regulator does not only accept the plans, but also influences the design process. This could also imply a decrease in undivided design authority in reducing power company autonomy.

'The authorities give us our marching orders for these things, we have to work according to that and also, [power plant name] has established their own guide-lines accordingly and, how the design work, what kind of documentation is required, so I'm not sure whether there's anything, they work well or don't, but we'll have to do them anyway. We cannot take any short cuts; we must follow the specified procedures. We cannot establish our own design methods in that sense.' (Energy company employee, the waste management system case)

In communicating with some power company workers, however, this issue of 'shared design authority' was promptly rejected: it was stated that the design authority clearly lies within the power companies. This could very well be true, but the current workers cannot speak on behalf of the future ones; if the plausible conditions for shared authority exist, the power companies should be conscious so that the responsibility of the end-product as a whole never slips away in daily design practices. This is indeed important because shared responsibility can sometimes mean that nobody takes the final responsibility of maintaining an overall understanding of the design process.

To summarize, the following possible causes imply that failing to maintain the understanding and responsibility of the overall project and end-product could be a plausible reason for unsuccessful designs in the NPP domain:

1. The threat of lack of focus on the end-product holistically due to the burdensomeness of documentation as well as project and requirements management.
2. The threat of sharing the design authority with the regulator, i.e., nobody would maintain the final and complete responsibility in actual design activities.
3. Technical complexity and the sheer size of some projects.

4 CONCLUDING INTERPRETATIONS: ACHIEVING RESILIENT DESIGNS?

This study is relevant in view of managing resilience as it discusses the shortcomings and trade-offs related to managing design in safety critical domains by stringent regulation and by increasing requirements – understanding the designed solutions holistically can be compromised due to the tediousness of requirement management and document drafting; yet, holistic understanding would be needed in creating resilient systems. We do not oppose thorough governmental regulation in safety critical domains, but, at the same time, one should ensure that gaining the regulator acceptance does not become the focus of design activity: safety and functionality should be the main design goals. Resilience engineering is to say that safety is not to be understood solely as the absence of accidents and other negative events but as a capability to perform successfully (Hollnagel et al., 2011). However, designing for capability of this kind can be in practice challenging if requirement management and precise document drafting are emphasized – this is because iteration of plans becomes more challenging; it might be hard to conceive how to operate a system in the best possible manner prior the first versions of the systems.

The argument thus goes that if the design activity focuses largely on technical requirement management and on drafting precise documents for the regulator, insufficient effort might be dedicated to iterating the design idea and to considering the design in terms of usage at a system level. Human activity would have to be considered holistically, however, if the system is to allow resilient and flexible activity; means for making sense of varied situations should be supported. These issues can be difficult to foresee in plans or to confine to requirements.

This study questions the thinking that increasing requirements and preciseness in regulation is a simple means for producing safety – other issues are needed as well. These include the following: 1) sufficient recourses for iteration and reconsidering the design idea, 2) safety culture in design, which emphasizes the design organization responsibility in lieu of regulatory acceptance, and 3) leadership that ensures system thinking in design. As discussed already, the first point seems to be well actualized in Finland, but may also reflect economic burdens in the domain. One could also consider the so-called 'incremental commitment model' in design, which has been proposed as an alternative to the already discussed V-model (Pew & Mavor, 2007). The key idea in the incremental commitment model is that the stakeholders involved evaluate different versions of the plans in different phases; these include initial scoping and concept definition. This implies that stakeholder opinion would be used in defining the initial plans and the design concept in the very beginning of the process. It could be problematic, however, if the regulator would participate at this phase with a formal role as a requirement specialist or such, because thus the regulator's independence as a reviewer could be compromised. The second and third point, in turn, reflect the DISC model of safety culture (Reiman et al 2009, Oedewald et al. 2011), which emphasizes responsibility for the entire system, seeing safety as a complex phenomenon, mindfulness, and management of good work conditions; the threats identified in this study could be understood as some of the issues the design organizations should be mindful about.

Overall, this article provides food for thought for those involved in design activities in a highly regulated safety-critical field. In order for the threats identified in our study not to take place, good and comprehensive requirements and rigorous regulatory oversight might not suffice; issues such as pride and feeling of responsibility in maintaining safety along with excellent and broadminded technical expertise and leadership are needed as well.

Acknowledgements

This study summaries and expands a chapter of a project report (Wahlström, in press). The study was supported by the SAFIR2014 programme, the Finnish State Nuclear Waste Management Fund (VYR), Nordic Nuclear Safety Research (NKS), VTT Technical Research Centre of Finland, and Vattenfall (Ringhals).

REFERENCES

Aspelund, K. (2006). *The design process.* New York, NY: Fairchild publications.

Hollnagel, E., Paries, J., David, D. W., & Wreathall, J. (2010). *Resilience engineering in practice: A guidebook.* Surrey, UK: Ashgate Publishing.

IAEA, (2003). *Maintaining the Design Integrity of Nuclear Installations Throughout Their Operating Life.* INSAG-19. Vienna, Austria: IAEA.

Macchi, L., Gotcheva, N., Alm, H., Osvalder, A.-L., Pietikäinen, E., Oedewald, P., Wahlström, M., Liinasuo, M. & Savioja, P. (2014). *Improving design pro-cesses in the nuclear domain. Insights on organizational challenges from safety culture and resilience engineering perspectives.* Final report, Nordic Nuclear Safety Research, NKS-301. Retrieved from http://www.nks.org/en/nks_reports/

Oedewald, P., Pietikäinen, E. & Reiman, T. (2011). *A guidebook for evaluating organisations in the nuclear industry - an example of safety culture evaluation*. Stockholm, Sweden: SSM.

Pew, R. W. & Mavor, A. S. (Eds.). (2007). Human-system integration in the system development process: A new look. Washington, DC: National Academy Press.

Reiman, T. & Oedewald, P. (2009). *Evaluating safety-critical organizations – emphasis on the nuclear industry.* Stockholm, Sweden: SSM.

Rollenhagen, C. (2010). Can focus on safety culture become an excuse for not rethinking design of technology? *Safety Science,* 48, 268–278.

Turner, R. (2007). Towards Agile Systems Engineering Processes. *CrossTalk, Journal of Defense Software Engineering,* 9, 11–15.

Wahlström, M. (in press). More requirements, more safety? Cultural tensions in NPP design activities. 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. 53–71). MANSCU Final report. VTT publications.

RESILIENCE CAPABILITIES

SAFETY AS AN EMERGENT PROPERTY OF THE PRODUCTION SYSTEM: WORK PRACTICES OF HIGH-PERFORMANCE CONSTRUCTION SUPERVISORS

Panagiotis Mitropoulos 1
1 San Diego State University, San Diego, California, USA
pmitropoulos@mail.sdsu.edu

Abstract

Construction work involves many dynamic and hazardous processes that are adapted to the project-specific requirements and context. Successful operational performance requires both high production and high safety performance. Thus, a significant challenge for construction researchers and practitioners is to develop resilient production systems that are simultaneously highly productive and highly safe under the demanding, complex, and dynamic conditions of construction projects. Towards this aim, this study investigated the work practices and principles of exceptional field supervisors who consistently achieve very high levels of both productivity and safety. The research used a case study approach. In-depth field studies documented the work management practices of exceptional supervisors in four high-risk construction trades—residential framing, masonry, concrete, and roofing). In each case, these practices were compared with the practices of an average performing supervisor from the same organization. The findings indicate that the exceptional supervisors used a combination of strategies that aimed primarily at preventing errors, rework and incomplete work. Their strategies included: (1) task management strategies that mitigated the task demands on the workers, and (2) crew management strategies that enhance the work group's ability to cope with high demands. The findings provide empirical evidence that the production practices that prevented errors are essential in preventing accidents. As a result, the safety performance was "an emergent property" of the production system.

1 INTRODUCTION

In 2013 the US construction industry employed 6% of all industries and had 20% of the fatal work injuries (Bureau of Labor Statistics 2015). Construction work involves dynamic and hazardous processes that are adapted to project-specific requirements and context. These processes combined with high production pressures and workload, create high potential for errors and accidents. A very dynamic environment is a key feature of hazardous work environments (Scarf et al 2001). Successful operational performance requires both high production and high safety performance. Thus, an important challenge for construction researchers and practitioners is to develop production systems that are highly productive and safe, and can function effectively in the dynamic and complex conditions of construction projects—in other words, they are resilient.

The current approach to accident prevention in construction is based on the normative paradigm. Safety programs focus on the control of hazards and aim primarily at increasing compliance with safety rules—they emphasize training, inspections and enforcement of safety requirements, and workers' motivation (Garner 2004). Efforts towards safety culture and behavior-based safety also aim at increasing the workers' voluntary compliance with prescribed hazard controls. This approach has contributed to the reduction of accidents, but it also has theoretical and practical limitations as it neglects the important role of production processes in the production of accidents.

The construction literature provides extensive evidence that the production system has a strong effect on safety performance (Suraji et al. 2001) argued that project conditions, design decisions or management decisions can cause responses that may lead to accidents. Hinze and Parker (1978) suggested that job pressures are more important than safety policies in preventing accidents. Studies of construction operations identified how project features and production practices influence the level of task demands on the workers (Saurin et al. 2008, Memarian & Mitropoulos 2013, and in press).

Rasmussen et al. (1994) describes how the production system shapes the behaviors and performance of the individuals in the system. Workers' behaviors tend to migrate closer to the 'boundary of loss of control' due to the production pressures for increased efficiency, and the tendency for least effort, which is a response to increased workload. Safety programs attempt to counter the above pressures and prescribe "safe behaviors" away from the boundary. However, the continuous pressures due to efficiency and workload result in a "systematic migration toward the boundary of acceptable performance (Rasmussen et al. 1994).

Production–safety trade-offs are an important element of the safety of production operations (Hollnagel 2009, Rasmussen 1997, Reason 1997, Mikkers et al 2012). Production employees make many large and small trade-off decisions every day (Woods et al 2010). Woods and Wreathal (2003) call them "sacrifice decisions." Hollnagel

2009 refers to the "Efficiency-Thoroughness Trade Off" (ETTO). The safety climate literature also recognizes the trade-offs between safety and production (Zohar 2000, Ford and Tetrick 2008, Das et al. 2008).

In construction, the organization of the production is typically performed by field supervisors (a. k. a. foremen) who operate within organizational, financial, and project constraints. The supervisors determine to a large extent the work structure, task allocation, sequencing, workload and pace, work coordination, controls, etc. In order to identify production practices that support both high production and high safety, this research investigated the work practices of exceptional field supervisors—that is supervisors who consistently achieve very high levels of both productivity and safety. These supervisors appear to successfully manage the efficiency-safety trade off in their operations.

2 METHOD

To understand the practices of exceptional foremen, the research used a case study approach and conducted in-depth field studies of selected supervisors. The practices of each exceptional foreman were compared to the practices of an average performing foreman from the same contractor. This involved extensive observations, interviews and discussions with many project participants (supervisors, workers, managers, safety professionals, etc.).

2.1 Research Activities

To identify HR foremen, each participating contractor evaluated their foremen based on the following: (1) Safety incident rate and severity over the previous three years, which was calculated based on the labor hours each foreman supervised, the number of incidents that occurred under their supervision, and the direct cost of incidents. (2) Production performance during the previous three years. This was evaluated using actual cost data (if available) or subjective data using the evaluation of the foremen by the company's operations manager. The assessment was based on the difficulty of the projects the foreman managed, and the foremen's productivity and schedule performance.

Interviews with the operations manager and safety manager were conducted to understand the organizational context, including the safety management policies, hiring policies, foremen and crew training, compensation and bonuses, work method selection, and foremen's level of decision-making regarding the work process. Safety incidents over the previous three years were reviewed to identify hazards and high-risk activities.

After securing the necessary permissions, the researchers performed extensive field observations and interviews with the selected supervisors, their crew members and other project personnel. About 20 site visits were conducted for each trade, including observations of average performing foremen. Operations were observed and often videotaped. The foremen were interviewed multiple times regarding all aspects of the work organization.

2.2 Cases

The study focused on trades with significant safety risk, as reflected in high rates of injuries and fatalities. This paper summarizes the findings from (1) residential framing, (2) concrete and (3) masonry supervisors.

The residential contractor employed about 85 framing crews. All crews performed very similar work in terms of complexity, size and schedule. The exceptional foreman was the one with the highest production score and zero incidents. The average foreman had productivity slightly above average, and incident rate just above the company average, and average workers' compensation cost. Both crews had 7 crew members. The masonry contractor performs residential, commercial and industrial work. The company employed more than 700 workers including about 60 foremen. The exceptional foreman was observed on a large project that involved several buildings. Another foreman was also on this project. Each foreman was assigned different buildings and each had a crew of 45-55 workers (2 masons to 1 laborer). The project had a complex design and an accelerated schedule. The concrete company was a large contractor who performs primarily commercial and industrial work. The contractor had about 20 supervisors. The selected supervisor was observed on a project that involved the construction of a 10-story office building, with a cast-in-place concrete frame and post-tensioned concrete slab. Each floor was 2,500 Square Meters. The design complexity was low. The main challenges were the tight schedule of 13 weeks and the high temperature. The supervisor was in charge of the entire concrete operation that included a deck crew (19 members), a wall crew (9) and a night crew (8).

3 FINDINGS

The findings indicate that the primary focus of exceptional supervisors was to prevent errors, rework and incomplete work. All their practices and strategies supported this guiding principle. Their strategies mitigated and balanced the demands of the task, as well as the capacity of their crew. An unexpected finding was that the safety

practices of high-performance foremen did not always involve extensive control of hazards and exposures.

Table 1. Production practices of high performance supervisors

***Guiding principle**: Prevent errors, rework and incomplete work*	
Task management strategies:	**Crew management strategies:**
• Organized the process for speed by completing smaller batches of work, overlapping activities and managing the dependencies. • Actively looked for production difficulties and risks, while the average supervisors operated largely based on repetition (do as before). • Simplified and standardized the activities to reduce complexity and physical demands. • Prepared the activities in detail to avoid production surprises and interruptions. • Mitigated the production pressures on their crews to prevent rushing and errors.	• Matched the manpower with the demands of the operation. • Kept the crews informed and focused. • The task assignments balanced the need for efficiency, with workers' learning and development. • Continuously monitored for errors, threats and difficulties, and responded fast to excessive workload and problems.

3.1 Guiding principle: Focus on preventing errors, rework and incomplete work

All high performing foremen had a strong focus on preventing errors, rework and incomplete work. For the framing foreman, the largest productivity losses happen when he has to go back and fix something. The masonry foreman emphasized that it is critical to have everything correct when he is finishing each area. Problems and mistakes are identified and corrected immediately and he rarely had any punchlist items. For the concrete supervisor, it was critical to avoid mistakes and delays, and to complete all the planned activities every day, in order to meet the aggressive schedule. This emphasis on avoiding mistakes and rework guided most of their work practices.

3.2 Task management strategies

Organizing the process for speed

The foremen organized the work process for speed by reducing the batch size, overlapping operations, and managing the dependencies. The masonry foreman divided the crew in smaller groups, who worked at different locations on the same floor. He focused on completing each area fast by assigning several masons in one area—masons were working closer together, which also reduced their walking "empty-handed. To accelerate the concrete operation, the supervisor divided each floor in two sections so the deck and walls operations could overlap. This overlapping created new resource dependencies: the concrete crews and crane. Each operation was assigned to a different crew so they could proceed independently. The dependency due to the crane was managed with better planning to reduce the number of lifts, and allocate the crane time to the different crews.

Anticipating threats and difficulties

The HR foremen were constantly looking for potential problems—difficult work areas, missing resources, coordination difficulties, mistakes and omissions. The framing foreman was always looking for details or options that his crew was not familiar with. He discussed them with the crew and asked them to wait for him before they start working on those **a**reas, to prevent errors. The masonry foreman was checking for complex block patterns, penetrations, and changes in the block that the crew needed to be aware of. The concrete supervisor was considering the potential difficulties of every activity, and actions to reduce them.

Design the activities to reduce complexity and physical demands

The foremen were looking for opportunities to simplify and standardize the work methods. The concrete supervisor selected methods and components that required less onsite assembly (aluminum tables configured for ease of installation), and less measuring and cutting ("Z metal" for the beam forms). He had the crew pre-mark the table legs to reduce measuring and prevent errors. When a wall involved complex block patterns, the masonry foreman had the block laid out in the correct order, to reduced complexity for the masons and prevent errors.

To reduce physical demands, the masonry foreman raised the scaffold more frequently to reduce cutting block due to rebar. The concrete crew used rubber mallets that deliver a softer blow and reduce the workers' discomfort. The framing foreman had little discretion regarding the material, method or tools—even then, he was using longer

than usual temporary braces for truss erection that made the installation easier. These strategies reduced the physical demands, and task complexity, which reduces the potential for errors.

Extensive preparations to reduce disruptions and delays

All high performance foremen put significant effort to ensure that the crew had all the material and resources needed to perform the work as planned. This was critical in order to avoid interruptions and incomplete work. The framing foreman checked if the lumber, hardware and trusses packages were complete and that no components were missing. The concrete supervisor assigned crew members dedicated to preparing the material, equipment, tools, for the activities. The masonry foreman checking all the material delivered, "knowing" that there was always something missing. He was also checking if the crew had on the scaffold everything they needed—the right block (type and color) and mortar, inserts, wire, ties, projection pieces, lintels or steel beam with all stirrups, etc. According to the masonry foreman, the ability to prepare the activities determined the number of work areas where he could work.

Mitigate production pressures

To prevent excessive pressures and workload the high performance foremen: (1) Set realistic production goals and tried to establish a pace that was not rushed. Having adequate manpower was an important consideration. The framing and concrete foremen had the authority to determine their crew size, and emphasized low absenteeism. Absenteeism was high in the masonry operation—the crew was "over-manned" by the management which was very tolerant to absenteeism. (2) Prepared tasks ahead of time (organized material in the order needed, pre-measured and pre-marked) to reduce pressures during installation. (3) "Shielded" the crew from being rushed by the following activities. The framing foreman was ordering the crane with a small time buffer to prevent it from arriving early and rushing his crew. The goal of these practices was to reduce excessive workload, rushing and fatigue, and reduce mistakes. However, when high pressures could not be avoided, the close monitoring enabled fast adaptations.

3.3 Crew management practices

The crew management practices of the high performing foremen aimed at preventing excessive workload, rushing and mistakes. Preventing absenteeism was critical for the concrete crew, as they were under time pressure and working overtime, and every absence would mean excessive workload for the rest of the crew. Absenteeism was high in the masonry operation, where the crew was "over-manned" by the management which was very tolerant to absenteeism. Crew planning was essential in keeping the crew informed and aware of their next step. Every day, the concrete crews reviewed the timetable, specifying what time each task had to be finished. The crew had a clear work plan which specified when, where, and how to do the work. To keep the crew focused, the workers were assigned one task at a time. In the masonry crew, the foremen and leadmen had very clear plans about what work to do, and they crew had clear directions and production goals.

The task assignments balanced the demands of the task with the crew capabilities. In the concrete crew, task rotation was used for some physically demanding tasks. Tasks that required high accuracy (in areas with low tolerance) were assigned to the most skilled carpenters. A leadman with strong engineering skills was performing the layout. A dedicated grader was used to set the table legs at the correct elevations. In the framing crew, only the leadman and another carpenter were allowed to perform the high risk tasks (setting trusses and install the first row of plywood). The masonry leadman and foreman prepared and checked the layout, and a dedicated group of four laborers was responsible for the scaffold.

The task assignments also supported workers' development. The masonry foreman was assigning the same tasks to the new workers as the experienced workers, so the new workers can learn how to perform all tasks. At the same time, he was assigning an experienced worker to monitor and correct the inexperienced ones. He also gave opportunities to crew members to take more responsibilities (e.g. oversee the rebar). The framing foreman framed the complex details himself and used them as an opportunity to train his crew members. the In the concrete operation, because of the very high schedule pressures, the supervisor assigned tasks based on the workers' capabilities, rather than learning opportunities.

Monitoring and cross-monitoring

The exceptional supervisors had close monitoring of both the task performance (in terms of progress and quality) and workers' conditions (such as fatigue, frustration, attention). They established multiple checks especially for critical operations where errors would be very costly. The framing foreman double checked the walls before they were lifted in place, and personally released the trusses during truss erection to ensure they were installed

correctly. For the masonry foreman, layout, block patterns and openings, and raising the scaffold were the activities with the high consequences of errors. He was continuously checking to identify and correct any mistakes before the crew left the work area. The concrete supervisor had established multiple checks for the elevation of the tables, and embeds, as well as several daily milestones to check progress.

Cross monitoring by the crew members was another strategy for identifying threats and difficulties. The concrete supervisor trained the crew to recognize the symptoms of dehydration and asked them to cross monitor each other for symptoms. Early recognition of mistakes and difficulties combined with a clear plan to address the problems made it possible for the crew to correct errors quickly or redistribute the workload. To prevent problems in one task affecting other tasks, the concrete crew was instructed to not stop their activity and help with production problems, but to notify the deck foreman immediately. The foreman knew the status of all tasks and redistributed the workload so that other tasks were not delayed.

3.4 Differences in safety management

Although all three supervisors had excellent safety performance, the three cases had significant differences in terms of the safety risks and control of hazards. The framing crew had limited safety measures and high exposure to hazards. Their most significant risks were falls from elevation, saw cuts and nailgun injuries. At the time of the study, the residential framing sector was exempt from conventional fall protection requirements. Consequently, the protection from hazards was limited and the exposures were high. The jobsites did not have a dedicated safety professional and the crew did not have safety toolbox talks.

For the masonry crew the most significant safety concerns were scaffold safety, saw cuts and heavy load lifting. A safety manager was assigned part-time on the project and safety toolbox talks were held once a week. For the tower scaffolds the masonry foreman had four laborers dedicated to inspecting, monitoring and raising the scaffold. Overall, the safety efforts were good but the remaining exposures to hazards were considerable. Scaffold inspection was performed daily.

The concrete operation had extensive safety measures to reduce exposures. The main safety concerns were falls, crane safety, falling objects during removal of the table forms, and dehydration. The crew had daily planning and safety meetings. Perimeter railing and 100% tie-off policy with zero tolerance were used to reduce exposures to falls. Crane activities were planned extensively and monitored closely. The risk of dehydration was mitigated by providing extra water and rotating workers to work in shaded areas. The safety measures significantly reduced the workers' exposures to hazards, and the exposures were relatively low.

The study resulted in some surprising findings with regards to safety management. First, although the high performing supervisors had exceptional safety, safety was not in all cases their top priority. Second, high safety performance was achieved even with minimal safety rules and controls, as the residential framing case highlights. Thus, high levels of safety were consistently achieved with greater emphasis on production controls, rather than hazard controls.

4 DISCUSSION

The study of high performance supervisors identifies production system design principles and practices that contribute to increasing the resilience of construction operations and work teams. The findings indicate that the production practices that prevented errors also prevented accidents. This underlies the nature of accident prevention as error prevention and management rather than hazard controls. In dynamic, uncertain work situations as in construction, where exposures to hazards are unavoidable, the ability to avoid errors is critical.

To reduce the likelihood of errors, exceptional supervisors use multiple strategies that (1) mitigate the task demands, and (2) keep the crew informed focused, and attentive. As a result, their work practices produce "**high quality" work situations**. The extensive preparations minimized unpredictable situations, and reduced unexpected problems (such as not having the right tools and material), frustration, rushing and errors. The management of production pressures reduced rushing, and the need for shortcuts or violations to meet production goals. At the same time, the crew management strategies prevented excessive workload and reduced distractions and frustration. The assignment of more capable personnel to more demanding tasks prevented overloading crew members with excessive task difficulty. The extensive monitoring increased the ability to recognize excessive workload and threats (such as fatigue or dehydration) and redistribute the load.

The findings support that safety is an emergent outcome of the production system design, rather than an outcome of compliance, or control of hazards. This investigation found that the production system is critical for safety because it generates the work situations that workers face. An ineffective production control system generates low quality work situations with excessive task difficulty and increased opportunities for errors and violations. Even with significant safety effort, there will be extensive friction with production, and the safety outcomes are likely to

be poor. This is not to say that strong safety efforts are not important, but they are not sufficient to overcome the problems of an ineffective production control system.

REFERENCES

BLS (2015) Revisions to the 2013 Census of Fatal Occupational Injuries (CFOI) counts, April, US Bureau of Labor Statistics http://www.bls.gov/iif/oshwc/cfoi/cfoi_revised13.pdf. accessed May 2015.

Das, A., Pagell, M., Behm M., and Veltri A. (2008) Toward A Theory of the Linkages Between Safety and Quality" J. of Operations Management 26 (2008) 521–535.

Ford, M.T., Tetrick, L.E., 2008. Safety motivation and human resource management in North America. The International Journal of Human Resource Management 19 (8), 1472–1485.

Garner, C. [2004] Construction Safety Program Essentials. In Construction Safety Management and Engineering (Darryl C. Hill, ed.), American Society of Safety Engineers.

Hinze, J., and Parker, H. W. (1978). "Safety, productivity and job pressures." J of the Construction Division, 104(1): 27-35.

Hollnagel E. 2009, "The ETTO: Principle: Efficiency Thoroughness Trade-Off. Why Things That Go Right Sometimes Go Wrong."Ashgate Burlington.

Mikkers, M., Henriqson, E. and Dekker, S. (2014) "Managing Multiple and Conflicting Goals in Dynamic and Complex Situations: Exploring the Practical Field of Maritime Pilots" J. Maritime Research 9(2): 13-18.

Mitropoulos, P. and Memarian, B. (2013) "Task Demands in Masonry Work: Sources, Performance Implications and Management Strategies" J. Constr. Eng. & Manage., 139(5): 581-590.

Memarian, B. and Mitropoulos, P. (in press) "Production Practices Affecting Worker Task Demands in Concrete Operations: A Case Study" WORK: A Journal of Prevention, Assessment, and Rehabilitation.

Rasmussen, J. (1997) "Risk management in a dynamic society: a modelling problem." Safety Scie 27(2):183-213.

Rasmussen J., Pejtersen A.M., and Goodstein L.P (1994). Cognitive Systems Engineering. John Wiley & Sons, Inc. New York, NY.

Reason, J. T. (1997). Managing the risks of organizational accidents (Vol. 6). Aldershot: Ashgate.

Saurin, T, Formoso C., Cambraia, F. (2008). "An analysis of construction safety best practices from a cognitive systems engineering perspective." Safety Science, 46(8): 1169-1183.

Scharf, T., Vaught, C., Kidd, P., Steiner, L., Kowalski, K., Wiehagen, B., Rethi, L., and Cole, H. (2001). "Toward a Typology of Dynamic and Hazardous Work Environments." Human and Ecological Risk Assessment, Vol 7 (7): 1827-1841.

Suraji A., Duff, A. R., and Peckitt S. J. (2001). "Development of Causal Model of Construction Accident Causation." J. Const. Eng. & Manage., 127(4): 337-344.

Woods, D., & Wreathall, J. (2003). Managing Risk Proactively: The Emergence of Resilience Engineering. Columbus: Ohio University.

Zohar, D., 2000. A group level model of safety climate: testing the effects of group climate on micro-accidents in manufacturing jobs. Journal of Applied Psychology 85 (4), 587–596.

ORGANISING HUMAN AND ORGANISATIONAL RESILIENCE AND RELIABILITY: RESEARCH PROGRAM AND APPLICATION FOR NUCLEAR POWER PLANTS ORGANISATION

Pierre Le Bot for the team MOREFOR

EDF R&D, 1 Avenue du Général de Gaulle, Clamart, France pierre.le-bot@edf.fr

Abstract

This paper will describe a research program focused on the organisational resilience and reliability of nuclear power plants' (NPPs) organisation. The characteristics of this program are:

- to gather a multidisciplinary team of specialists involved in different EDF's projects,
- to start from EDF's experience in various domains of nuclear operation,
- to take into account internal issues and developments about resilience such as the MRS model and the international state of the art
- to provide the different EDF's projects with contributions using the concept of organisational resilience and reliability, leading to operational results.

In a paper for the 2015 PSAM conference the author proposed a generalisation of the model called the Model of Resilience in Situation (MRS) which is coherent with the Resilience Engineering Approach and the High Reliability Organizing Approach.

Initially the MRS was built empirically from simulators observations of emergency operation of NPPs. It was theoretically based on the Theory of Social Regulation by J.D. Reynaud. The model supports the Human Reliability Analysis EDF's method MERMOS. In the model, resilience is the ability of the organisation to combine dynamically in situation both robustness and autonomy by alternating them whenever needed. The anticipation process contributes to the organisational abilities of resilience and robustness. The adaptation process contributes to the organisational abilities of resilience and autonomy. The three organisational abilities of resilience, robustness and autonomy allow the Safe Operation and allow the organisation to be reliable. The entire organisation can be described in a global loop of linked processes, if the previously mentioned processes (adaptation, anticipation and operation) are completed by taking into account the Organisational Learning.

The added value of the MRS is for example to show how both rationalities underpinning the anticipation process and the adaptation process must coexist and can coexist in a reliable organisation even if they are often opposite. Moreover, the resulting ambiguity and the resulting conflicts of the coexistence of these rationalities are unavoidable to obtain Safety. A second example is that expertise, which is different from training, is needed to get autonomy in order to be adaptable and consequently resilient.

The research program aims at sketching a general model taking into account the MRS. It will also integrate other relevant models for, and from, organisational assessments and actions in different EDF's internal projects. In the multidisciplinary research team, risk analysis specialists, ergonomists, sociologists and human and organisational reliability analysts will share their former experience and the feedback from their contribution to the projects. The team is called MOREFOR (MOdèle de Résilience et Fiabilité ORganisationnelle).

The MRS model considers resilience as the ability to combine dynamically in situation both robustness and autonomy by alternating them whenever needed. The MOREFOR research program will investigate how resilience is obtained from anticipation and adaptation that are using the Organisational Learning. In this way it proposes a frame of thinking in accordance with the topic of the Symposium "Managing resilience, learning to be adaptable and proactive in an unpredictable world".

DIVIDE AND CONQUER STRATEGIES FOR ENHANCED RESILIENCY IN ELECTRICAL TRANSMISSION LINES

Shaleena Jaison [1], D. Subbaram Naidu[2] and Jake P. Gentle[3]
[1] Idaho State University, 921 South 8th Avenue, Pocatello, Idaho, U.S.A
[1] Email: jaisshal@isu.edu; Ph: +1(208)220-6602
[2] University of Minnesota Duluth, 1023 University Drive, Duluth, Minnesota, USA
[2] Email: dsnaidu@d.umn.edu ; URL: http://www.d.umn.edu/~dsnaidu
[3] Idaho National Laboratory, Idaho Falls, Idaho, U.S.A
[3] Email: jake.gentle@inl.gov

Abstract

With the modernization of the existing electric grid with smart grid technology, overhead power transmission lines have to be monitored in real-time to meet energy demands. Even though smart control and decision making characterize this technology, it's increasing dependence on cyber infrastructure makes its vulnerable to cyberattacks. The control strategies in place have to protect the transmission system from perturbations/faults as well as be resilient to cyber-attacks. In this paper, an optimal control scheme is presented that mitigates perturbations in a transmission line (TL) and is resilient to outages/attacks. This design exploits the inherent time scale nature of transmission lines. Time Scale Analysis methods are applied to decouple the slow and fast dynamics in a TL, resulting in lower order, slow and fast subsystems. Linear Quadratic Regulators are designed separately for each subsystem. The simulations compare the proposed method to a full order system and also check the stability of the control design in the event of failures. The results manifest the effectiveness of the proposed method, which provides comparable control with reduced order subsystems, and also provide stability of the transmission system in the absence/failure of one of the controllers.

1 INTRODUCTION

The energy demands of the modern world and extreme weather conditions have brought about high stresses on the existing energy infrastructure. Power outages due to severe weather conditions are likely to increase in the future as the climatic changes are altering the frequency and intensity of natural events [U.S. DOE, August 2013]. These growing concerns have led to the research and development of smart electric grids which could provide real time monitoring and control of the existing power resources.

Decisions to manage power, such as diverting excess power from a less demand to a high demand area, increasing ampacity levels of existing transmission lines based on real-time weather conditions [Gentle, *et.al.* 2015], etc. will be part of controller strategies to meet daily power demands. Safety and stability of the power system has to be ensured at all times, and this requires the controller to mitigate any perturbations or faults in the transmission line (TL) and return power to nominal levels. With smart grid technology, software control and decision making becomes deeply integrated into the electric power system. However, the increased dependence on cyber infrastructure makes it vulnerable to malicious cyber-attacks. Hence, to improve the security of the smart grid, control strategies have to be devised that are resilient to faults and malicious attacks.

In this paper, an optimal control design is proposed that mitigates perturbations in a TL, and which incorporates resiliency as part of its design. The resiliency arises from having a decentralized control scheme with multiple controllers instead of one central controller, thereby ensuring the stability of the whole system in the event of failure of one of the controllers. This control realization is possible due to the slow-fast behaviour of the TL dynamics.

The organization of this paper is as follows: Section 2 presents time domain modelling of transmission lines, which captures the electrical and thermal dynamics in a TL. The slow-fast dynamics is verified through state

response plots and linearizations. In Section 3, Time Scale Analysis is carried out where the full order TL system is decoupled into slow and fast subsystems, independent of each other. LQR design using time scales is presented in Section 4 where controllers for mitigating system perturbations, are designed separately for each subsystem. Section 5 presents the results and conclusions of the proposed LQR for perturbation control and system stability in the event of failure of one of the controllers.

2 TIME DOMAIN MODELING OF TRANSMISSION LINES

A non-linear model of a TL is provided in this section. A short length line, described using a lumped parameter model, is considered for analysis and its equivalent circuit is as shown in Figure 1. The resistance of the transmission line, R is a function of conductor temperature, T_{avg} and it determines the amount of current flowing through the line.

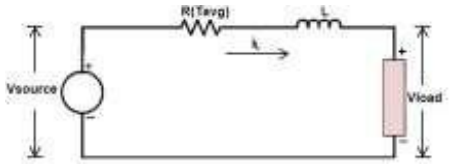


Figure 1. Equivalent circuit of a short-length transmission line

Transmission lines are subjected to various events in the field. Few of which that cause a noticeable impact are, current flow in the line, heating effects due to line resistance, weather effects on the line, for example cooling due to wind flow or heating due to increase in ambient temperature. The temperature dynamics in a TL is well described in the IEEE Standard 738 [IEEE-738, 2012]. However, it fails to address the line current dynamics that occurs simultaneously with the temperature dynamics. In this model, a TL is modeled as a complex system where both the line current dynamics and temperature dynamics are simultaneously present and interact with each other. The current dynamics is described using Kirchoff's current and voltage laws, while the temperature dynamics is described using [IEEE-738, 2012]. The state space model is provided in (1) as,

$$\begin{aligned}\frac{di_L(t)}{dt} &= -i_L(t)\frac{R(T_{avg})}{L} - i_L(t)\frac{R_{load}}{L} + \frac{v_{source}}{L},\\ \frac{dT_{avg}(t)}{dt} &= \frac{1}{mC_p}\left[R(T_{avg}(t))i_L^2(t) + q_s - q_c - q_r\right],\end{aligned} \tag{1}$$

Where $i_L(t)$ is the current flowing through the circuit, $T_{avg}(t)$ is the average temperature of the line conductor which depends on the line current (i_L), solar heat gain (q_s), convection heat loss (q_c) and radiation heat loss (q_r). m is mass per unit length of the conductor, C_p is the specific heat of the conductor material, L is the line inductance, R_{load} is a resistive load at the receiving end of the line, and v_{source} is the source voltage. The definitions of $R(T_{avg})$, (q_s), (q_c) and (q_r) are defined in the [IEEE-738,2012]. The nonlinear model in (1) is expressed in the standard nonlinear form, $\dot{\boldsymbol{x}} = f(\boldsymbol{x},\boldsymbol{u})$, where the state vector $\boldsymbol{x}$ and input vector $\boldsymbol{u}$ are,

$$\boldsymbol{x} = \begin{bmatrix} i_L & T_{avg}\end{bmatrix}^T,\ \boldsymbol{u} = \begin{bmatrix} v_s\end{bmatrix} \tag{2}$$

2.1 Analysis of the Transmission Line Model

The nonlinear model was simulated to capture the time scale nature of transmission lines. The system was perturbed by a step change in source voltage at the origin, and the state responses were observed. The plots of states with respect to time are displayed in Figure 2.

It was observed that the line current's step response was much faster than that of the line temperature. Observing the rise time of current near the origin, revealed it to be in the order of milliseconds, while that of temperature was in the order of minutes. This difference in the speed of variables indicates the presence of two time scales in the system, one slow and one fast. To further investigate, the nonlinear system was linearized about various operating points and the eigenvalues were evaluated. The results are tabulated in Table 1. The clearly distinct eigenvalues at any time instant signifies that transmission lines exhibit time scales, where the line current dynamics operate on a fast time scale and the temperature dynamics operate on a slower time scale.

Since time scale behaviour was observed, a transmission line is an ideal candidate for Time Scale Analysis. In the following section, the full order transmission line model is decoupled into lower single order, slow and fast subsystems, for which separate LQR controllers are designed.

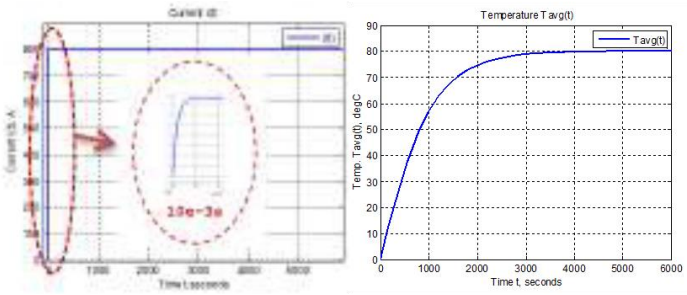


Figure 2. Response of line current and line temperature to a step change

Table 1. Linearization of transmission line model at various time instants

Time instant	Eigenvalues
t = 0s	-2.6561*10^3; -2.6102*10^-4
t = 1000s	-2.6682*10^3; -1.4177*10^-3
t = 2000s	-2.6712*10^3; -1.4478*10^-3
t = 3000s	-2.6719*10^3; -1.4551*10^-3
t = 6000s	-2.6866*10^3; -1.4901*10^-3

Singular Perturbation and Time Scale Analysis methods are well recorded in literature and its applications span various fields of engineering. These methods offer model order reduction and significant computational savings, which facilitates online implementation of controllers [Naidu D. S., 2002].

3 TIME SCALE ANALYSIS METHOD

A brief description of the decoupling process into a slow and fast subsystem [Naidu & Calise, 2001] is mentioned below.

The nonlinear model in Section 2 is linearized about an operating point as,

$$\begin{aligned} \dot{x}_1 &= A_{11}x_1 + A_{12}x_2 + B_{11}u, \\ \dot{x}_2 &= A_{21}x_1 + A_{22}x_2 + B_{21}u, \end{aligned} \tag{3}$$

Where x1 and x2 are the m- and n- dimensional state vectors, u is an r-dimensional control vector, and matrices Aij and Bij are of appropriate dimensions. This linear system should have widely separated groups of eigenvalues.

3.1 Decomposition of System Dynamics

A two-stage linear transformation [Naidu & Calise, 2001], given by

$$x_s = x_1 - Mx_f\,,\; x_f = x_2 + Lx_1\,, \tag{4}$$

is applied on the system in (3) to decouple it into independent slow and fast subsystems,

$$\begin{aligned} \dot{x}_s(t) &= A_s x_s(t) + B_s u(t), \\ \dot{x}_f(t) &= A_f x_f(t) + B_f u(t), \end{aligned} \tag{5}$$

where,

$$\begin{aligned} A_s &= A_1 - A_2 L, & A_f &= A_4 + LA_2\,, \\ B_s &= B_1 - MLB_1 - MB_2\,, & B_f &= B_2 + LB_1\,. \end{aligned} \tag{6}$$

The subscripts 's' and '*f*' denote slow and fast states respectively. The matrices A_1 to A_4 and B_1 to B_2 are obtained from the equations in (3) as,

$$A_1 = A_{11}, A_2 = A_{12}, B_1 = B_{11}, A_3 = A_{21}, A_4 = A_{22}, B_2 = B_{21} \tag{7}$$

The variables $L(n \times m)$ and $M(m \times n)$ are solutions of the nonlinear Lyapunov-type equations,

$$\begin{aligned} LA_1 + A_3 - LA_2L - A_4L = 0, \\ (A_1 - A_2L)M - M(A_4 + LA_2) + A_2 = 0. \end{aligned} \tag{8}$$

which are calculated iteratively using the high accuracy Newton method [Gajic & Lim, 2001]. It is evident from (5) that the state variables x_s and x_f can be solved independently of each other. In the full order system, the slow and fast dynamics interact with each other which causes 'stiffness' in computations. The decoupled systems are relieved of 'stiffness' and hence provide significant computational savings.

3.2 Time Scale Analysis Results

On linearizing the model equations in (1) about a nominal operating point, 2nd order system matrices were obtained.

$$A = \begin{bmatrix} \underset{A_3}{0.0001684} & \underset{A_4}{-0.001462} \end{bmatrix}; B = \begin{bmatrix} \underset{B_2}{0} \end{bmatrix}$$

L and M were calculated iteratively using Newton's Algorithm. The 1st order decoupled matrices were found to be,

$$A_s = [\text{-2687}]; \; A_f = [\text{-0.0010289}] \qquad B_s = [25.39]; \; B_f = [\text{-2.2658e-05}]$$

To ensure that the decoupled systems retain the slow and fast dynamics, the eigenvalues of the full order and reduced order systems were compared. The eigenvalues are provided in Table 2. The results confirm that the time scale method decouples the system dynamics almost perfectly. The accuracy parameter of Newton's algorithm could be adjusted to get the exact same eigenvalues for both the systems.

Table 2. Comparison of full order and reduced order eigenvalues

Full Order	**Eigenvalues**
A	eig(A) = -2687; -0.0014924
Reduced Order	**Eigenvalues**
A_s - slow subsystem	eig A_s = -2687
A_f - fast subsystem	eig A_f = -0.0010289

4 OPTIMAL CONTROL DESIGN

In general, an optimal controller provides the best possible performance for a given performance index or cost function. When the performance index is quadratic, and the optimization is over an infinite horizon, the resulting optimal control law obtained by minimizing the cost function is called Linear Quadratic Regulator (LQR). Transmission lines are subjected to perturbations arising from sudden loading effects by a set of electric motors, or a lightning strike to the line, or an abrupt change in the source voltage. In such events, the objective of an LQR control is to bring the perturbed states to zero. It is assumed that all the states are measurable and the control signal is unconstrained for design purposes. The performance index is chosen to minimize the error between the perturbed state and the desired state (which is zero) for an infinite time period.

4.1 LQR Control Design

Generally, the standard LQR design for any full order system does not separate the slow and fast dynamics.

Here we propose a LQR design for the decoupled transmission line where control laws are implemented separately for the slow and fast subsystems [Jaison *et.al.*, 2014].

The slow subsystem x_s defined in (5), has a performance index, P_s is the solution of the slow algebraic Riccati equation

$$J_s = \frac{1}{2}\int_{t_0}^{\infty}\left[x_s^T(t)Q_s x_s(t) + u_s^T(t)R_s u_s(t)\right]dt, \tag{9}$$

where Q_s and R_s are the weighting matrices for the slow subsystem. The control signal $u_s(t)$ for the slow subsystem is calculated as:

$$u_s^*(t) = -K_s x_s(t) = -R_s^{-1}B_s^T P_s x_s(t), \tag{10}$$

where K_s is the regulator gain of the slow subsystem and equation,

$$P_s A_s + A_s^T P_s + Q_s - P_s B_s R_s^{-1} B_s^T P_s = 0. \tag{11}$$

Similarly for the fast subsystem, the LQR control is calculated as,

$$u_f^*(t) = -K_f z_f(t) = -R_f^{-1}B_f^T P_f x_f(t). \tag{12}$$

where P_f is the solution of the fast algebraic Riccati equation,

$$P_f A_f + A_f^T P_f + Q_f - P_f B_f R_f^{-1} B_f^T P_f = 0. \tag{13}$$

A block diagram describing LQR control design for the reduced order transmission line is presented in Figure 3. The feedback control is a composite control $u^*(t)$ i.e. sum of slow control $u_s^*(t)$ and fast control $u_f^*(t)$.

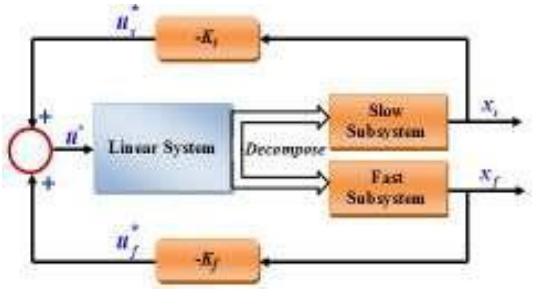


Figure 3. LQR control design for reduced order linear transmission line

4.1 Resilience of LQR Control with Time Scale Approach

Resilience of controller operation is of paramount concern in today's highly interconnected and networked society. In the event of a cyber-attack or failure of a controller, especially for critical and sensitive applications, implementing a decentralized control scheme will be highly beneficial. This would guarantee some control action to be still in place which would avoid critical failure of the entire system. In the event of controller outages, it may be possible to control the plant/system using any one of the multiple controllers designed. Such a control system designed to tolerate failures of controllers, while retaining desired control system properties, is a "reliable" control system.

The decoupling of slow and fast dynamics in a transmission line facilitates implementation of a decentralized control scheme. Here, it is shown how a single controller (either slow or fast) by itself gives nearly original performance, thereby making the system more reliable or 'resilient' in case of either controller malfunction.

The linear transmission line was tested for three cases:

- Control signal = slow control + fast control
- Control signal = only slow control
- Control signal = only fast control

5 RESULTS & CONCLUSIONS

All the controllers were designed in MATLAB® and implemented in Simulink®. Model data for simulations were taken from [IEEE-738, 2012] for a 795 kcmil 26/7 Drake ACSR conductor.

5.1 Results of LQR Control

Matrices A_s, B_s, A_f and B_f for LQR control design were provided in Section 3.2. The weighting matrices Q_s, R_s, Q_f and R_f were chosen such that they minimize the time taken by the states to get to zero. These matrices were chosen from multiple iterations. A comparison between the full order and reduced order control of linear transmission line is provided in Figure 4.

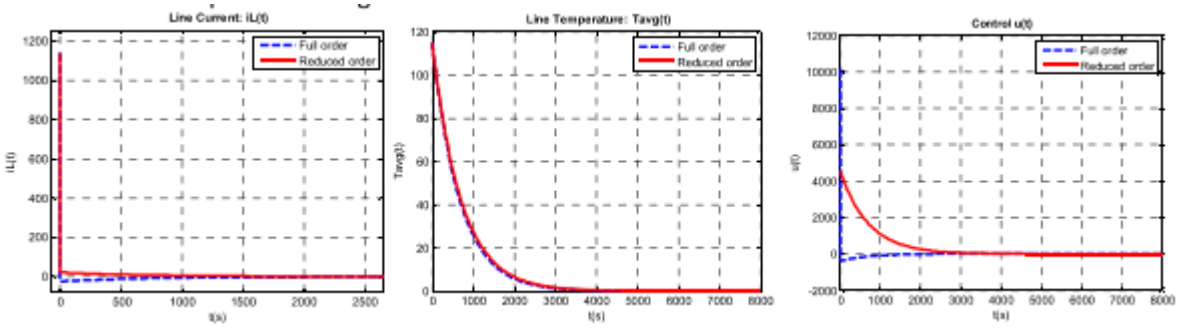


Figure 4. States and control of linear transmission line model

It was observed that the controller regulates the states to zero, for both full order and reduced order cases. The very close matching between the full order and reduced order LQR control manifests the effectiveness of the time scale method. Thus the proposed method provides almost the very same control action with less computational effort. This implies that lower order controllers could be implemented online for applications that demand real-time monitoring and control.

5.2 Stability of Transmission Line with Two Controllers

The results of simulation for the three cases of control inputs mentioned in Section 4.2 are given in Figure 5.

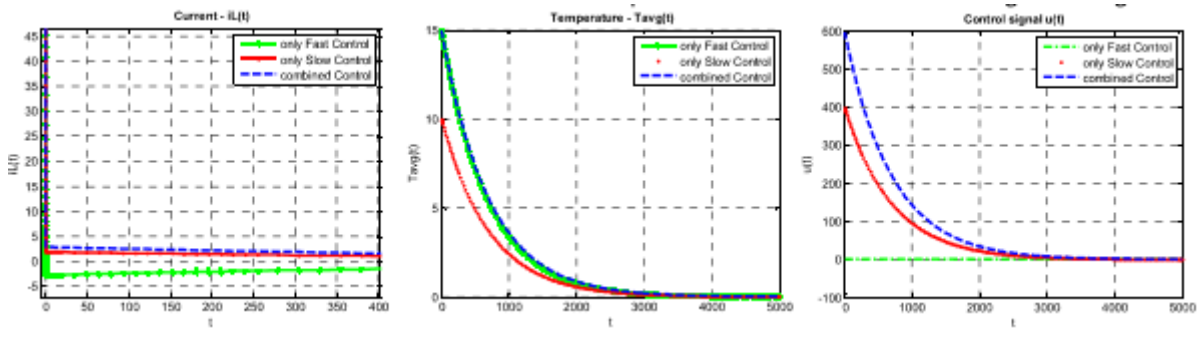


Figure 5. Comparison of state responses to single control input and combined control input

The last plot shows the 3 cases of control inputs. The 1st two plots display the response of current and temperature states to the three control inputs. It is observed that the states' response to the single control input (either slow or fast) is very close to that of the combined control input. This shows that even in the absence/failure of one of the controllers, the remaining control effort does provide comparable control to the whole system. This reiterates the strength of the time-scale control design approach, which provides (multiple controllers) resiliency to the systems as compared to a centralized control design.

6 CONCLUSIONS

A time domain modelling approach was presented to capture the electrical and thermal dynamics of transmission lines. This model renders instantaneous values of line current and line temperature, which are very useful information for Dynamic Line Rating of transmission lines. These instantaneous values when fed to an operator or a decision making controller, would help establish the safe line ampacity levels based on real- time conductor temperature.

Time scale techniques were presented that facilitated simpler controller designs to mitigate system perturbations. The simulation results confirm that comparable control action can be delivered with separate lower order slow and fast controllers. In a real scenario where various components of a power system chain are modelled (typically comprising of generators, transmission lines, power electronic interface dynamics, etc.), the combined model order could be very high, and controller design/online implementation, becomes computationally challenging. With the proposed time scale approach, higher order systems could be reduced to lower order subsystems, based on the number of time scales present in the entire system. Lower order models offer significant computational savings, and facilitate online control implementations. Finally, it was demonstrated that the presence of multiple controllers in place of one central controller guarantees comparable control action during failure of one of the controllers in the system, thereby ensuring resiliency and stability of the transmission system.

REFERENCES

Gajic, Z., & Lim, M. (2001). Optimal control of singularly perturbed linear systems and applications- High accuracy techniques. New York: Marcel Dekker, Inc.

Gentle, J. P., Parsons, W. L., West, M. R., & Jaison, S. (2015). Modernizing An Aging Infrastructure Through Real-Time Transmission Monitoring. 2015 IEEE Power & Energy Society General Meeting. Denver, CO.

IEEE-738. (2012). IEEE Standard 738 - Standard for calculating the current temperature relationship of bare overhead line conductors.

Jaison, S., Naidu, D. S., & Zydek, D. (2014). Time Scale Analysis and Synthesis of Deterministic and Stochastic Wind Energy Conversion Systems. WSEAS Transactions on Systems and Control, 189-198.

Naidu, D. S. (2002). Singular perturbations and Time Scales in Control Theory and Applications: An Overview.

Dynamics of Continuous, Discrete and Impulsive Systems Series, 9(Series B), 233-278.

Naidu, D. S., & Calise, A. J. (2001). Singular perturbations & Time Scales in Guidance and Control of Aerospace

Systems: A survey. Journal of Guidance, Control and Dynamics, 24(6), 1057-1078.

U.S. DOE. (August 2013). Economic Benefits Of Increasing Electric Grid Resilience To Weather Outages.

energy.gov. Retrieved from energy.gov

MANAGING RESILIENCE THROUGHOUT THE NUCLEAR POWER PLANT LIFECYCLE: THE SIGNIFICANCE OF PRE-OPERATIONAL PHASES

Nadezhda Gotcheva [1], Pia Oedewald [2], Kaupo Viitanen [2] and Mikael Wahlström [2]
[1] VTT Technical Research Centre of Finland, P.O. Box 1300, FI-33101 Tampere, Finland
[1] E-mail: nadezhda.gotcheva@vtt.fi, Tel. +358 40 132 6030
[2] VTT Technical Research Centre of Finland, P.O. Box 1000, FI-02044 VTT, Espoo, Finland www.vtt.fi

Abstract

The objective of this paper is to explore how cultural challenges in the pre-operational phases of a nuclear power plant project (e.g. design, construction and commissioning) create prerequisites for development of resilience in latter phases of the project. Organizational processes and practices, beliefs, assumptions and understanding about safety developed in one lifecycle phase might not be fully relevant for the next phase. The study indicates that challenges in different phases are related to the extent of tangibility of the nuclear safety concept, magnitude of technical and organizational project complexity, extent of subcontracting, organizing of the project activities, or the priority given to nuclear-specific knowledge and understanding. Resilience management approaches should take into account the different cultural features of the lifecycle phases and how they affect safety. Accordingly, the means to support resilience should be adapted according to the specific cultural challenges in each phase. The paper highlights the significance of the pre-operational phases for making informed decisions to create and manage resilience throughout the nuclear power plant lifecycle.

1 INTRODUCTION

Many activities in contemporary large-scale nuclear energy projects are carried out by complex networks of multinational actors. Networks are seen as a dynamic set of actors who collaborate to achieve shared goals and generate value (Camarinha-Matos et al., 2009). However, the diversity of perspectives in large projects brought by multiple project partners often brings tensions, fragmentation and power issues. Although actors generally agree upon the core goals of the project, they might not share the same goals and priorities due to different roles, responsibilities and perspectives. Also, compared to single organizations, in temporary project networks it is more difficult to hold actors accountable for results and safety performance.

A general intrinsic challenge in the nuclear industry is ensuring the long lifespan of an operational nuclear power plant, which brings requirements for modernizations, maintaining mindfulness, managing the effects of aging, or preparing for internal or external turbulences. Provided that the lifetime of nuclear power plants encompass several decades and beyond, the relevance of resilience as a long-term ability to adapt and thrive in the face of changes and uncertainty is evident. The range and nature of activities in large-scale nuclear energy projects bring new challenges for creating and managing resilience. Resilience Engineering tradition sees resilience as the intrinsic ability of an organisation to adjust its functioning prior to, during, or following both expected and unexpected changes and disturbances (Hollnagel et al., 2011). The core resilience abilities to anticipate, monitor, respond and learn developed during one lifecycle phase might be dysfunctional in the next phase due to changes in the characteristics of the system. This could be referred to different organizational core task of each phase (i.e. the shared objective or purpose of organizational activity), associated hazards, ways of organizing and competence requirements (Reiman & Oedewald, 2007).

The *research question* to be addressed in this paper is how cultural challenges, identified in the pre- operational phases set conditions, which might affect the development of resilience in latter phases of the lifetime. The focus of this study is on pre-operational phases, more specifically, design, construction and commissioning, since they offer valuable opportunities to identify and correct possible issues *before* the operational phase actualizes. For example, it has been recognized that decisions taken during the design phase might have significant consequences on, e.g. maintenance, waste handling and the costs for final decommissioning of the plant (IAEA, 2002).

The paper summarizes and extends a research, which utilized international reports, scientific publications and the authors' experience from empirical evaluations in different lifecycle phases in large-scale nuclear power projects on safety culture and organizational projects (Gotcheva & Oedewald, 2015).

2 LIFECYCLE MANAGEMENT IN COMPLEX NUCLEAR POWER PLANT PROJECTS

The lifecycle of a new nuclear power plant consists of five phases (Fig. 1), such as pre-project, project decision-making, construction (including design, construction, installation and commissioning), operation and decommissioning phases, which can be grouped into pre-operational, operational and post-operational phases (IAEA, 2007; 2012).

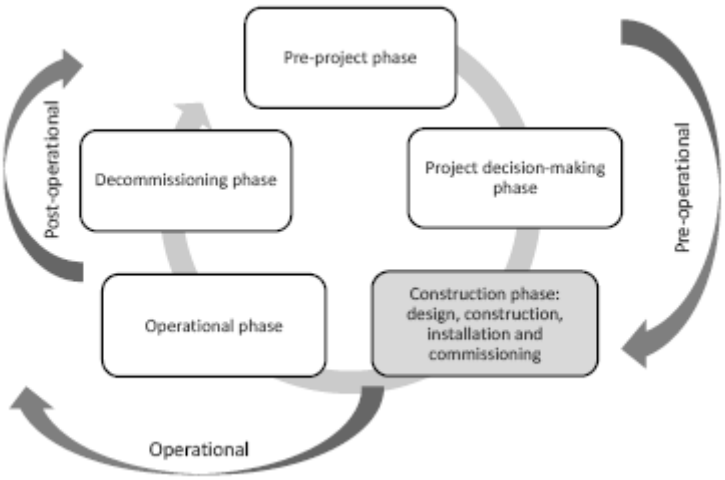


Figure 1.Nuclear power plant's lifecycle (based on IAEA, 2007)

This paper focuses explicitly on design, construction and commissioning activities, which are seen as a part of the construction phase in the nuclear power plant's lifecycle. In the pre-operational phases of a large nuclear project multitude of organizations from different nationalities and professional backgrounds are involved in a broad range of activities. These are usually subcontractor organizations, which might have very limited nuclear experience and insufficient knowledge of nuclear safety requirements, and often speak different languages, which create challenges for coordination, management, accountability and communication (IAEA, 2012). In the pre-operational phases the nuclear fuel and associated hazards are absent from the site until the initial fuel loading, which challenges the relevance of applying the safety culture concept.

Traditionally, the concept of safety culture in nuclear domain has been associated with nuclear hazards; therefore it may be difficult to understand its relevance in phases where nuclear fuel is not present. Safety culture is seen as an organization's potential for safety (Reiman & Oedewald 2009, Oedewald et al. 2011). If safety culture principles and practices are not adequately understood and applied from the very beginning of the project, there is a risk of latent and actualized deficiencies, project management issues, and overall safety issues during operation of the plant, which applies to both new nuclear build and big modernization projects in existing plants (Ruuska et al., 2011; IAEA, 2012). Recent research indicated that problems related to quality assurance, coordination and communication in early phases of large construction projects tend to cascade and manifest in the later construction phase (Albrechtsen & Hovden, 2014). Current experience in the Nordic nuclear industry sector points out that there are challenges associated with creating and sustaining a good safety culture during the pre-operational phases (e.g. Oedewald & Gotcheva, in press; Oedewald et al., 2011b; Gotcheva et al., 2014; Macchi et. al, 2014).

Main challenges associated with safety culture during pre-operational phases of large nuclear power projects were identified by IAEA (2012) as follows: 1) many organizations with limited direct experience and insufficient knowledge of nuclear safety requirements may be involved in various activities at the site; 2) a wide range of

organizations are typically involved in pre-operational activities, which poses challenges for coordination, management and accountability; 3) projects may involve many different nationalities and cultures, which can result in communication challenges; and 4) new build nuclear power plant sites may be located in countries with no mature nuclear industry, nuclear knowledge and infrastructure, or in countries with a mature industry but with limited or no recent experience.

These issues bring complex interrelations and localized adaptations, which have the potential to aggregate and to generate emergent phenomena or system-wide patterns, which should be anticipated and managed (Eoyang & Holladay, 2013). Nuclear power plant projects can be seen as complex adaptive systems (CAS), since they represent a collection of semi-independent agents, in which inputs are not necessarily proportional to outputs, and which have the ability to learn and adapt to changes (McMillan, 2008). These systems are highly sensitive to their initial conditions: the so called "butterfly effect" implies that small differences in the initial conditions can lead to a wide range of outcomes.

In that sense, what works in one lifecycle phase cannot be simply replicated in another phase because each one has distinct characteristics. Crosby (2012) studied building resilience in large high-technology projects and indicated that early adoption of certain approaches and launch conditions have the capacity to position a project for resilience in its later phases of the lifecycle. For example, paying attention to "front-end shaping", which builds resilience by alignment of all parties with a common objective and setting launch conditions, such as a clearly defined mission, clear reporting and decision structures, preparation for unexpected risks and awareness of the external environment, as well as establishing deliberate support for collaborative relationships and structures, including contractors. This implies that we need to better understand the initial characteristics and typical human, organizational and cultural challenges, experienced in the pre-operational phases of the lifecycle in order to create potential for creating and managing resilience throughout the whole lifecycle.

3 CULTURAL CHALLENGES DURING PRE-OPERATIONAL PHASES OF NUCLEAR POWER PROJECTS

The following sections summarize the main results; that is, the cultural and organizational challenges that arise in the different lifecycle phases of a nuclear power plant project (for a more detailed report on safety culture challenges in large nuclear projects see Gotcheva & Oedewald, 2015).

3.1 Design phase

Design in the nuclear industry is a *collective process and coordinated effort between multiple parties*, such as the licensee, the regulator, the vendor and a large network of design organisations, which sets demands on collaboration activities, sharing of responsibilities and communication concerning safety requirements and priorities. Distributing roles and responsibilities between different stakeholders in design is challenging, especially in the beginning of a project when relationships and organisational structures are still establishing. Design involves effective *requirements management*: identifying, finding, understanding and implementing various requirements. In addition, national regulatory requirements should be thoroughly understood by foreign designers. When multiple organizations are involved, designers' sense of responsibility for safety and functioning of the end-product may be challenged due to their physical or psychological distance from the end-users and their local context, which poses a risk for suboptimal solutions. This implies that to develop resilient design, a culture which encourage open reporting of safety or quality concerns should be developed. Besides, designers' knowledge on the broader context and use of the systems in the plant should be enhanced. It is difficult to standardize the conceptual stage of design with detailed instructions and requirements. There is a large amount of requirements and their interpretations among designers might differ. There is a need to *manage tensions and to develop a systemic view* in design, including technical and non- technical understanding such as materials behaviour, end user's needs and future operational context. Psychologically, in this phase nuclear safety is a distant concept, which may contribute to a limited sense of responsibility for the end-product and the overall plant safety.

3.2 Construction phase

In the construction phase it is challenging to ensure that the large number of actors, e.g. subcontractors, in a complex temporary multinational network have a sufficient safety understanding. Provided that the majority of the construction subcontractors usually work in non-nuclear domain, where the requirements and vocabulary are different, it is not easy to understand what is safe and what is unsafe, especially when immediate nuclear hazards are not yet present at the site. Also, when multinational workforce in involved in the construction field, language and cultural barriers could complicate understanding of the need to follow procedures and nuclear specific requirements, which could compromise safety. Therefore, collaborative relationships with contractors need to be supported and developed, especially since the construction context is highly dynamic: the constant flux of companies and workers disturbs the process of shared learning through training and knowledge transfer. Another challenge is that traditionally, construction industry is focused on occupational safety rather than on system

safety. Construction industry utilizes hierarchical management model, which emphasises bilateral interactions and information exchange and focus on efficiency, which might have undesirable effects on safety.

3.3 Commissioning phase

Commissioning is a critical phase in the nuclear power plant lifecycle because it aims at demonstrating and verifying that the constructed components, systems and structures are operational and done in accordance with the design specifications (IAEA, 2014). Unidentified deficiencies in this nuclear safety critical phase could remain major latent failures for a long time after the reactor starts operation (Zerger and Noël, 2011). Dealing with possible deficiencies during the commissioning phase requires deep knowledge, prompt and prudent judgement and managerial excellence (Cagno et al., 2002).

Commissioning involves more tangible safety risks compared to design and construction insofar as loading of nuclear fuel is part of commissioning. After the fuel loading, the commissioning tests require the same attention to nuclear safety as during the operational phase. In this phase, fragmented problem solving process might impede communication and coordination, and cloud the big picture. Hence, integration of activities and management of the unexpected are required during the commissioning process because of the increased organizational and technical complexity. Commissioning activities require a deep understanding of the nuclear specific quality requirements, which makes it different from construction work since the hazards of the nuclear fuel are present at the site after the fuel loading, and the systems are actually used, not only constructed or designed; the empirical findings stemming from using the systems need to interpreted against the design basis.In addition, the increased organizational and technical complexity requires a systemic view for dealing with expected and unexpected conditions.

4 DISCUSSION

To enhance the overall resilience of the future plant, it is important to understand how the pre-operational lifecycle phases of a nuclear power plant project create prerequisites for developing resilience in the next phases. Hence, the discussion focuses on the lifecycle phase interactions and the possible relations to the resilience cornerstones.

The *design* phase sets some of the key preconditions for self-organising later in the project. If this effect is not considered, e.g. by means of including end-users who actually operate the plant in design activities, the designers may not understand or anticipate correctly how the system will evolve and self-organise when it is taken into operation. Design is also incorporating lessons learned from previous experiences concerning the nuclear power plants. Active involvement of the licensee and the regulator early in the design process is critical for anticipating the risks for costly and time-consuming design changes, which might have effects on safety in the later phases. The design solutions are crucial for the capability for monitoring and responding as well, yet the designers need to understand how these activities should be carried out and integrated in the design process. Organizational systems and structures should support the coordination and shared learning between different stakeholders in the design process, such as the licensee, the regulator, design organizations, external consultants, subcontractors, etc. Safety should be made a more tangible concept for designers, and thus improving their sense of responsibility for the final outcome and the overall plant safety.

In the *construction* phase there are multiple interactions between a large number of actors in the project, which creates preconditions for patterns of coordination to arise out of the local interactions in a highly dynamic context. Construction provides opportunities to monitor if there are needs for modifications in case of weak or dysfunctional design solutions, which could jeopardize safety of the future power plant. The resilience development approaches should take into account the challenge of prioritizing quality and safety in a context of multitude of international construction workers, who are typically involved in non-nuclear industries. Thus subcontractors need to be involved and supported in understanding the nuclear specific hazards, since otherwise their ability to anticipate potential risks and react adequately to disruptions could be diminished.

In the nuclear industry, *commissioning* refers to proving the resilience of a safety-critical system before it is put in operation. In a way, the commissioning phase “acquire” the conditions of the plant, shaped by the developments during the design and construction. The activities are focused on noticing and fixing possible deficiencies from the previous phases, and testing the components and systems against design and safety requirements. Anticipating the potential safety impacts of specific actions or decisions during commissioning requires solid knowledge in technical characteristics, hazards and system behavior. This cornerstone of resilience may be challenging to achieve when utilizing subcontractors in safety critical activities. Learning from past experiences and understanding of the big picture actualizes in commissioning phase because there is a need to verify that the systems are safe. The safety risks related to the nuclear fuel loading stage bring pressure for dealing with the

unexpected, just like in operational plants. The increased social and technical complexity in this phase requires effective coordination and clear roles and responsibilities. From resilience cornerstones perspective it can be stated that during commissioning there is a need to create an ability to anticipate how the plant will function in the future, develop organisational capabilities for monitoring and responding to expected and unexpected plant behaviors. Overall, this process can be seen as a learning journey, which is documented carefully and often under time pressure.

Organisations evolve dynamically throughout their lifetime and are often characterised as being sensitive to initial conditions. This notion could be applied also to complex nuclear power plant projects. The resilience abilities developed during one lifecycle phase might prove to be dysfunctional if applied directly in the next phase. For instance, organizations might have developed practices to respond to certain conditions during the construction phase, such as the huge number of subcontractors from different nationalities, which might be dysfunctional for the commissioning phase, where there are typically less staff and less foreign subcontractors involved. Learning from past events can be problematic in project-based organizations since there might be not sufficient time to reflect, to communicate and to share experiences among different actors due to the temporal context and changes of personnel. It can be argued that although each of the lifecycle phases affects the overall resilience of the future power plant, the pre-operational phases set conditions, which influence significantly the long-term ability of the actors in a project network to continuously adjust to or recover from changes and disturbances.

5 CONCLUSION

This paper highlighted the significance of pre-operational phases for developing resilience throughout the nuclear power plant lifecycle by pointing to the need to capture the dynamics of the pre-operational phases and develop an understanding on the cultural challenges that might have an effect on safety. Organisations evolve dynamically throughout their lifetime and are often characterised as being sensitive to their initial conditions. Understanding the characteristics, behaviour of the system and the challenges organizations face early in the lifetime allow making informed decisions to create and manage resilience in latter phases. This understanding supports the timely and sufficient development of system capabilities for safety and coping with varying conditions throughout the lifecycle. In other words, this enhances the ability of organizations to recognize outdated practices and to develop flexibility to revise the relevance of communications, decision processes, procedures and systems during each lifecycle phase. In this paper we argue that the culture, which steers the way workers think and behave in latter phases of the lifecycle, is set in the pre-operational phases, and it includes the formation of structures and practices, values, attitudes, knowledge and understanding. Changing this interlocking set of cultural features is a large-scale and long-time undertaking. Therefore, if from the beginning an organization is developed in a dysfunctional way, it might be more difficult to manage resilience in the later phases. Since organizational challenges differ between the phases, the means to support and sustain resilience might need to adapt accordingly.

Acknowledgements

The work presented in this paper is based on research projects supported by the Finnish Research Programme on Nuclear Power Plant Safety (SAFIR2014), the Swedish Radiation Safety Authority (SSM) and the Finnish Radiation and Nuclear Safety Authority (STUK). The authors are grateful to the power companies for their cooperation and support during the case studies.

REFERENCES

Albrechtsen, E. & Hovden, J. (2014). Management of emerging accident risks in the building and construction industry, In Proceedings of Workingonsafety.net, 7th international conference, 30 September-03 October 2014, Scotland, UK.

Cagno, E., Caron, F. & M. Mancini (2002). Risk analysis in plant commissioning: the Multilevel Hazop. *Reliability Engineering & System Safety*, *77*(3), 309-323.

Camarinha-Matos, L.; Afsarmanesh, H; Galeano, N. & Molina, A. (2009). Collaborative Networked Organizations, *Computers and Industrial Engineering*, *57*(1), 46-60.

Crosby, P. (2012). Building resilience in large high-technology projects: front end conditioning for success, *International Journal of Information Technology Project Management, 3*(4), 21-40.

Eoyang, G. & Holladay, R. (2013). *Adaptive action. Leveraging uncertainty in your organization*. Stanford University Press, Stanford.

Gotcheva, N. & Oedewald, P. (2015). SafePhase: Safety culture challenges in design, construction, installation and commissioning phases of large nuclear power projects, February, 2015:10, ISSN 2000-0456, Swedish Radiation Safety Authority (SSM).

Gotcheva, N., Oedewald, P., Macchi, L., Alm, H., Osvalder, A.-L. & Wahlström, M. (2014). Managing safety culture in design activities: Evidence from the Nordic nuclear power domain; presented at the WOSNET 2014, 7th international conference, 30 September - 03 October 2014, Glasgow, Scotland, UK.

Hollnagel, E., Paries, J., Woods, D. & Wreathall, J. (Eds.) (2011). *Resilience Engineering in Practice: A Guidebook*. Ashgate.

IAEA (2002). *Safe and Effective Nuclear Power Plant Life Cycle Management towards Decommissioning*, IAEA, Vienna, IAEA-TECDOC-1305.

IAEA (2007). *Managing the First Nuclear Power Plant Project*, IAEA-TECDOC-1555. Vienna: International Atomic Energy Agency.

IAEA (2012). *Safety Culture in Pre-Operational Phases of Nuclear Power Plant Projects*. Safety Reports Series No. 74. Vienna: International Atomic Energy Agency.

IAEA (2014). *Commissioning for Nuclear Power Plants*, Specific Safety Guide, No. SSG-28. Vienna: International Atomic Energy Agency.

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 organizational challenges from safety culture and resilience engineering perspectives, Final report, Nordic Nuclear Safety Research, NKS-301.

McMillan, E. (2008). *Complexity, Management and the Dynamics of Change*. London: Routledge.

Oedewald, P. & Gotcheva, N. (in press) Safety culture and subcontractor network governance in a complex safety critical project, Reliability Engineering and System Safety, Special Issue "Resilience Engineering".

Oedewald, P., Gotcheva, N., Reiman, T., Pietikäinen, E. & Macchi, L. (2011b). Managing safety in subcontractor networks: The case of Olkiluoto3 nuclear power plant construction project. 4th Resilience Engineering International Symposium, Sophia-Antipolis, France, 8-10 June.

Oedewald, P., Pietikäinen, E. & Reiman, T. (2011a). *A guidebook for evaluating organizations in the nuclear industry – an example of safety culture evaluation*, SSM: The Swedish Radiation Safety Authority, 2011: 20.

Reiman, T. & Oedewald, P. (2007). Assessment of complex sociotechnical systems: theoretical issues concerning the use of organizational culture and organizational core task concepts. *Safety Science, 45*(7), 745-768.

Reiman, T. & Oedewald, P. (2009). Evaluating safety critical organizations: focus on the nuclear industry. Swedish Radiation Safety Authority, Research Report 2009:12.

Ruuska, I., Ahola, T., Artto, K., Locatelli, G. & Mancini, M. (2011). A new governance approach from multi-firm projects: lessons learned from Olkiluoto 3 and Flamanville 3 nuclear power plant projects. *International Journal of Project Management*, *29*, 647-660.

Zerger, B. & Noël, M. (2011). Nuclear power plant commissioning experience. *Progress in Nuclear Energy*, *53*(6), 668-672.

IT, SYSTEMS AND NETWORKS

RESILIENCE AND NETWORKS

Jan Maarten Schraagen[1,2]
[1]TNO Earth, Life, and Social Sciences, P.O. Box 23, 3769 ZG Soesterberg, Netherlands
jan_maarten.schraagen@tno.nl
[2]University of Twente/BMS/CPE, P.O. Box 217, 7500 AE Enschede, Netherlands
J.M.C.Schraagen@UTwente.nl

Abstract

The purpose of this paper is to apply network science to the field of resilience engineering. Starting with the trade-off between prepared versus deliberated knowledge, I argue that socio-technical systems are first and foremost networked systems that need to connect modules of prepared knowledge or instances of deliberated knowledge by means of protocols. I hypothesize that particular frameworks for organizing protocols, or 'architectures', are more resilient than others. In network science terms, protocols are interaction patterns that may lead to sustained adaptability in the face of unexpected events. Research in a variety of domains has shown that scale-free network structures, with a power-law degree distribution, have the highest resilience. The relevance of this finding for social networks and for the concept of resilience as sustained adaptability remains to be demonstrated. It is clear, however, that social network analysis in particular, as a novel research methodology in this field, offers a more quantitative base to establish resilience engineering research upon.

1 THE PREPARATION VERSUS DELIBERATION TRADE-OFF

One of the main issues within the field of resilience engineering is the question how systems deal with surprise events. More generally, systems are able to perform under a variety of conditions by drawing upon a mix of prepared knowledge or deliberated knowledge (Newell, 1990). Prepared knowledge facilitates the recognition of familiar events and results in efficient, robust, and rule-based performance. Deliberated knowledge is required when systems are confronted with surprise events. In this case, the emphasis is on thoroughness and analysis of multiple options. The variety of situations leads to a specific mix of deliberation and preparation, and the architecture of a specific system determines the extent to which a response stems from deliberation or preparation. Humans, for instance, generally rely on prepared knowledge, as demonstrated by the finding that at least 80% of their decisions are recognition-primed rather than analytical. The human cognitive architecture, as well as the externally fixed time to respond, simply do not allow for much deliberation. Intelligent computer systems have different architectures and are able to engage in extensive search, comparing millions of situations per task, but generally have little prepared knowledge to bring to bear.

There is thus a preparation versus deliberation trade-off that has been known for some time for intelligent systems (see Newell, 1990) and is depicted below:

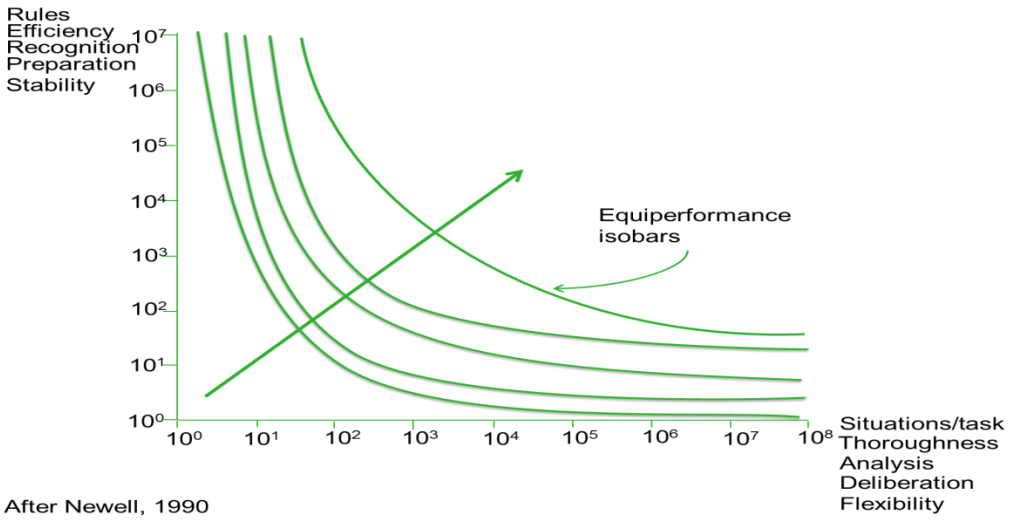


Figure 1 Preparation versus deliberation trade-off (after Newell, 1990)

Figure 1 shows that different systems may reach the same performance (on a single equiperformance isobar) by a different mix of either preparation or deliberation. The arrow denotes the optimal-mix points where cost-isobars (not depicted) touch the highest-performance isobar. These points constitute best trade-offs between amount of problem search and amount of knowledge search.

It is also clear from figure 1 that resilient performance should be in the area depicted by the optimal-mix points, along the arrow. Humans, taken as individual intelligent systems, are positioned in the top-left quadrant (lots of preparation, little deliberation), which results in robust, yet fragile (Doyle et al., 2005) behavior. Automated systems are positioned in the bottom-right corner (lots of deliberation, little preparation), which results in flexible, yet vulnerable behavior. The bottom-left corner is the brittle zone where systems run a high risk of saturation (Woods, 2015). The top-right corner is the area far from saturation where resilience should be positioned. The question is what architecture allows a system to balance the preparation versus deliberation trade-off (Woods, 2015).

2 MODULES AND PROTOCOLS AS THEY RELATE TO RESILIENCE

The concepts of 'modules' and 'protocols' may now be added to explain how systems deal with surprise events. Originally developed by Doyle and Csete (2002) in the area of biological systems and later extended to engineered systems, modules are defined as well-structured layers with high internal complexity that display robust behavior, while protocols are the rules that describe allowed interfaces between the modules. Protocols are generally fixed and small in number compared to modules, but they are the most vulnerable to attacks by viruses and other parasites. Modules may be compared to packets of prepared knowledge that yield robust behavior in the face of familiar events, but may fail catastrophically in the face of surprise events. In the face of surprise events, therefore, we need protocols to connect various modules in order to arrive at a less fragile response pattern.

Network science deals with the description of phenomena in terms of nodes and edges/arcs (relations or links between nodes). From a network perspective, modules are the nodes, whereas protocols are the links between the nodes. In social networks, protocols provide the information flow that is necessary to connect modules of prepared knowledge (information is taken to be an external phenomenon, whereas knowledge is an internal phenomenon; see Zins, 2007). I hypothesize that in order to be resilient, unrestrained information flow is a necessary condition. Particular frameworks for organizing protocols, and thus for managing information flow in networks, are more likely to demonstrate sustained adaptability than others (Woods, 2015).

From a cognitive science perspective, adaptive systems are what they are from being ground between the nether millstone of their physiology or hardware and the upper millstone of a complex environment in which they exist (Simon, 1980). To paraphrase Simon (1980), networked systems are what they are from being ground between the nether millstone of their limited channel bandwidth, which sets inner limits on their adaptation, and the upper millstone of a complex environment, which places demands on them for change. Networked social systems are capable of adapting to complex environments, but hardly ever perfectly. They could be called 'resilient' if they would demonstrate sustained adaptability over longer scales (Woods, 2015), but the reality is that most networked systems do not. Just as cognitive systems are boundedly rational, due to information processing limitations, networked systems are boundedly resilient, due to channel bandwidth limitations. These limitations are partly hardwired, but are also partly due to variations in absorptive capacity, centralized network position, tie strength, trust, and shared vision and systems (Van Wijk, Jansen, & Lyles, 2008). These factors have demonstrable positive effects on organizational knowledge transfer, yet can also impede knowledge transfer when they are less well developed.

If resilience engineering is taken to be the study of networked systems that operate in an unpredictable world, then the search for relative invariants must be found in the inner and outer environments that bound the adaptive processes. The inner environment of networked systems poses constraints on the types of information that can be transmitted. One relative invariant that has been found is the diversity-bandwidth trade-off (Aral & Van Alstyne, 2011), stating that high diversity of information exchange inevitably results in low channel bandwidth, whereas low diversity of information exchange results in high channel bandwidth. Resilience may be viewed as managing the trade-off between increasing a diversity of perspectives versus increasing homogeneity of perspectives. A choice within this trade-off space is determined by characteristics of the outer environment, such as the time available to reach a decision. Increasing a diversity of perspectives may be required when ample time is available, in situations where it pays off to be proactive, for instance in planning teams. A deliberate choice for increasing homogeneity of perspectives may be required in situations of time pressure, when it pays off to be highly responsive, for instance in action teams. This trade-off is similar to the trade-off many organizations face—that between exploration of new possibilities versus exploitation of known opportunities (March, 1991). As Rivkin and Siggelkow (2007) have shown, the patterns of interaction that exist in organisational, social and technological systems strongly determine how much to invest in long-run exploratory efforts. For instance, a centralized pattern of interaction results in a few decisions and the remaining choices are obvious, thus further exploration is not required. On the other hand, a

dependent structure, in which a handful of decisions are affected by virtually every other decision, yet those decisions exert very little influence themselves, will substantially benefit from exploratory activities. Rivkin's and Siggelkow's (2007) study indicates that particular network structures may determine the long-term resilience of complex systems.

3 EMPIRICAL EVIDENCE FOR RESILIENT ARCHITECTURES

Given that we live in an unpredictable world, the question is how we prepare for and anticipate surprise events. By studying examples of organizations that have done so successfully, we may gain insights in successful architectures, taken in Doyle's sense of 'frameworks for organizing protocols'. I will make a first attempt at answering these questions by providing illustrative examples from various domains, ranging from technical to social systems.

3.1 Supply network disruption and resilience

Kim, Chen, and Linderman (2015) recently studied supply network disruptions from a network-level perspective. A supply network can be viewed as a collection of nodes (facilities) and arcs (transportation linking facilities). A disruption of a node or an arc sometimes has little effect on the supply network, but at other times can bring down the entire network. Kim, Chen and Linderman (2015) define supply network resilience as "a network level attribute to withstand disruptions that may be triggered at the node or arc level" (p. 50). Resilience is therefore an emergent structural property of a supply network that has to do with the extent to which a network stays connected.

Kim, Chen and Linderman (2015) studied four basic supply network structures that frequently occur in real-world supply chain management settings and that each may have different degrees of resilience: block-diagonal, scale-free, centralized and diagonal (see Rivkin & Siggelkow, 2007 for more detail and other network structures). To calculate supply network resilience for each of these four network structures, the authors randomly removed nodes and arcs and estimated the likelihood of a network disruption. The results showed that the *scale-free* network structure had by far the highest resilience. Denser networks and networks with the most walks were not the most resilient. Also, the network level metrics of betweenness centrality and centralization did not correlate with resilience. These results suggest that *degree distribution* of a supply network plays a critical role in determining its resilience. In particular, networks that display a power-law distribution are likely to be more resilient. In networks with a power-law distribution, most nodes lie on few paths between others. Therefore, random node/arc removal rarely affects the overall connectedness of a network with this structure, as already shown by a large body of research initiated by Albert, Jeong, & Barabasi (2000).

3.2 Resilience in industrial symbiosis networks

Industrial symbiosis networks are networks of industries that use each other's waste and by-products to achieve a mutually beneficial relationship. For instance, a power plant and refinery may use groundwater and surface water for industrial purposes, while the power plant may in addition use seawater as cooling water for electricity production. Subsequently, wastewater and the cooling water are reused as well as recycled within industries to reduce the extraction of groundwater and surface water. Chopra and Khanna (2014) studied the industrial symbiosis network at Kalundborg, Denmark and used network metrics and simulated disruptive scenarios to understand the resilience of this network. They were also interested in how the network developed over time, from 1960 to 2010. They found that a single node in the network, the Asnaes power plant, was the most central and therefore critical. Time trends revealed, however, that the network became less susceptible to single points of failure over time. Chopra and Khanna (2014) found a pattern of preferential attachment, as new industries that joined primarily attached themselves to the Asnaes power plant. This results in a network structure that has a power-law degree distribution. As mentioned in the previous paragraph, these networks tend to be robust to random removal of nodes, but they are vulnerable to targeted removal of central nodes (Albert, Jeong, & Barabasi, 2000).

3.3 Resilience in medical and military teams

By using social network analysis techniques, my colleagues and I have gained insight in the communication structures at the team level, and have related these dynamic structures to the demands of the environments in which the teams operate. For instance, we have studied the response of a paediatric cardiac surgical team to surprise events (Schraagen, 2011; Barth, Schraagen, & Schmettow, 2015) and found that communication patterns are dynamically adjusted in the face of such events (communication becomes less hierarchical and more heedfully interrelated). We have also studied the network structures displayed by this particular team as a function of the phase in the surgical procedure, for instance whether the patient was going on or off cardio-pulmonary bypass (a highly critical phase in the cardiac surgical procedure that requires close cooperation between the surgical team members). We found that in any given phase, there were always two team members linked to many others, thus scoring high on total degree centrality. Not surprisingly, the primary surgeon was always one of these, with the

anaesthetist and perfusionist being the second actor, depending on the surgical phase. We also looked at complex versus non-complex procedures and found that during complex procedures the role of the assisting surgeon increased relative to the role of the primary anaesthetist, especially when going on or off cardio-pulmonary bypass. Although the primary surgeon still scored highest in total degree centrality in virtually all cases, the assisting surgeon filled in the role of communicator to the rest of the team whenever the workload of the primary surgeon prevented him from speaking to the rest of the team. This form of 'heedful interrelating' (Schraagen, 2011) shows that this team is at least adaptive, if not resilient. It is also a very important observation vis-a-vis the Albert, Jeong, & Barabasi (2000) finding that scale-free networks are highly vulnerable to targeted attacks. Capable people, such as the assisting surgeon, may compensate for the virtual 'elimination' of the most connected node in the network, the primary surgeon, whenever he is overloaded. Note that the assisting surgeon only took over the communication processes, while the primary surgeon continued with the physical work.

So far, we have not looked in detail at the precise structure adopted by this team. However, the results clearly display a power-law distribution of the total degree centrality, for both complex as well as non-complex procedures (see figure 2), leading us to suspect that this team displays a scale-free network.

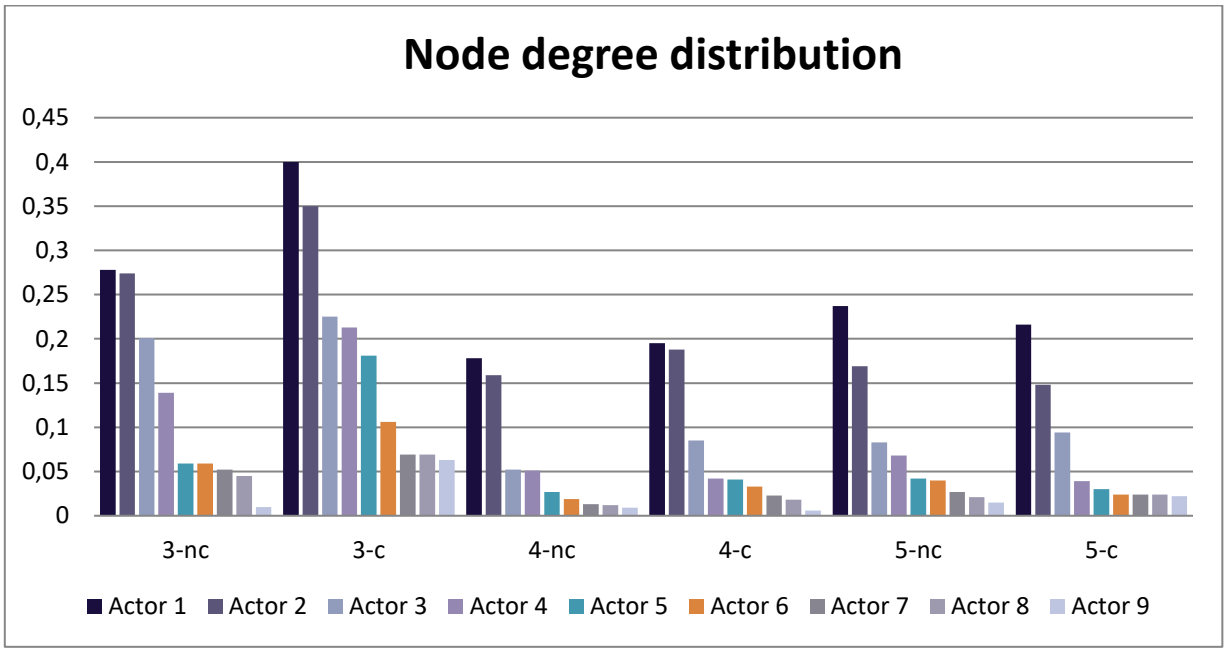


Figure 2 Distribution of total degree centrality for each node (medical actor) in the network. The figure only shows the three most critical phases in the surgical procedure (3-5), for both non-complex (nc) and complex (c) procedures

As a second example, a study of communication patterns in two separate naval internal battle teams showed that the more experienced team displayed more centralized communication patterns than the less experienced team, an example of a protocol evolving over time (Schraagen & Post, 2014). The central actor in the more experienced team, the Resource Manager, displayed significantly higher scores on total degree centrality than the other actors, as compared to the less experienced team. Most significantly, however, is the fact that distribution of total degree centrality displays a power curve for the more experienced team compared to the less experienced team (see figure 3), again suggesting a scale-free network structure.

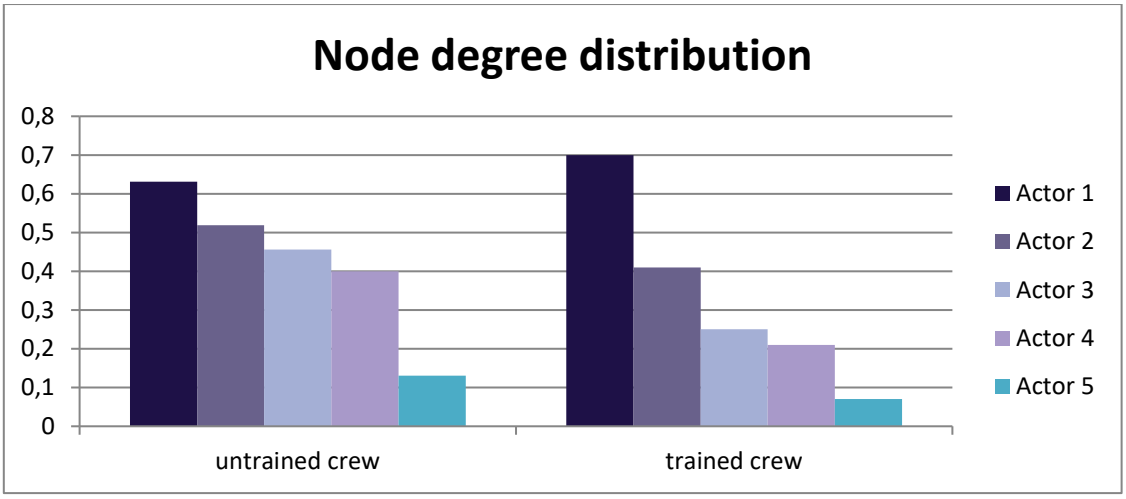


Figure 3 Distribution of total degree centrality for each node (military actor) in the network, for both the untrained crew (left) and the trained crew (right)

4 CONCLUSIONS

Complex socio-technical systems are first and foremost networked systems. In order to achieve their goals, these systems will select information from their networks using a limited number of protocols. Resilient performance in such systems is characterized by the flawless selection of such protocols, delivering information to the nodes in the network as needed to respond to a variety of conditions. Surprise events will be dealt with at local levels (through prepared knowledge or processes of improvisation) to the largest extent possible, thus maintaining the flow of the operation at the higher level. In a variety of domains, scale-free network structures have been shown to be resilient architectures, in the sense of being robust to the (random) removal of nodes. Specifically, in such resilient architectures the degree distribution of nodes follows a power law. This provides a direction for future research in resilience engineering, as it focuses attention to protocols and network characteristics of resilient networked systems. Moreover, it provides an impetus to the empirical investigations of such network structures using techniques such as social network analysis (Barth, Schraagen, & Schmettow, 2015).

However, we have also seen that there is a difference between social networks on the one hand and physical or biological networks on the other hand. Due to the adaptability of people in social networks, the results obtained with simulation models and random removal of nodes and arcs in physical networks may not generalize to social networks. Thus, the Robust Yet Fragile (Doyle et al., 2005) nature of many large-scale complex physical networks may be dampened in social networks, as people are flexible in taking over each other's roles, provided there are sufficient levels of trust and mutual understanding.

The question remains why we found that the degree distribution of nodes followed a power law in our social systems (at the team level), just as was found for the physical systems discussed. It may well be that this finding is a consequence of limited bandwidth constraints on human communication, making it simply impossible for actors to maintain communication links with many other simultaneously. A scale-free network may be the natural consequence of such constraints rather than a cause of resilience or sustained adaptability.

What, then, does resilience have to do with particular network structures? We hypothesize that this particular structure is able to deal with disturbances that are not well modelled, unexpected events that an OR team or a naval team such as we have studied needs to deal with as the occasion arises. In our research on communication processes within the OR, we have shown that the medical team adapted its communication structure to the external task demands, such as the complexity or the phase of the procedure (Barth, Schraagen, & Schmettow, 2015). In fact, the team blended a bureaucratic structure, with a central role for the surgeon, with a flexibility-enhancing structure, adding team members to the surgeon as the situation demanded. This results in a small-world or scale-free network structure, where supporting actors such as the anaesthetist, perfusionist or assisting surgeon switch roles in being the second-most-linked actor depending on the surgical phase. Also, the team as a whole adopted a flatter structure as procedures became more complex. We believe therefore that, in fact, these are network architectures that can sustain the ability to adapt to future surprises as conditions evolve (Woods, 2015). Future research needs to show whether scale-free networks are better able to deal with fundamental trade-offs such as the diversity-bandwidth trade-off than other architectures. It may very well be that there is a curvilinear relationship between scale-free

networks and performance, such that too much connectivity may decrease the level of diversity of information exchanged (Uzzi & Spiro, 2005).

REFERENCES

Albert, R., Jeong, H., & Barabasi, A.-L. (2000). Error and attack tolerance of complex networks. Nature, 406, 378-382.

Aral, S., & Van Alstyne, M. (2011). The diversity-bandwidth trade-off. *American Journal of Sociology, 117(1),* 90-171.

Barth, S., Schraagen, J.M.C., & Schmettow, M. (2015). Network measures for characterizing team adaptation processes. *Ergonomics*. DOI:10.1080/00140139.2015.1009951

Chopra, S.S., & Khanna, V. (2014). Understanding resilience in industrial symbiosis networks: Insights from network analysis. *Journal of Environmental Management, 141*, 86-94.

Csete, M.E. & Doyle, J.C. (2002). Reverse engineering of biological complexity. *Science, 295*, 1664-1669.

Doyle, J.C., Alderson, D.L., Li, L., Low, S., Roughan, M., Shalunov, S., Tanaka, R., & Willinger, W. (2005). The "robust yet fragile" nature of the Internet. *Proceedings of the National Academy of Sciences, 102,* 14497-14502.

Kim, Y., Chen, Y.-S., & Linderman, K. (2015). Supply network disruption and resilience: A network structural perspective. *Journal of Operations Management, 33-34*, 43-59.

March, J.G. (1991). Exploration and exploitation in organizational learning. *Organization Science, 2,* 71-87.

Newell, A. (1990). *Unified theories of cognition*. Cambridge, MA: Harvard University Press.

Rivkin, J.W., & Siggelkow,N. (2007). Patterned interactions in complex systems: Implications for exploration. *Management Science, 53(7),* 1068-1085.

Schraagen, J.M.C. (2011). Dealing with unforeseen complexity in the OR: The role of heedful interrelating in medical teams. *Theoretical Issues in Ergonomics Science, 12(3),* 256-272.

Schraagen, J.M.C., & Post, W.M. (2014). Characterizing naval team readiness through social network analysis. *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting* (pp. 325-329), Chicago, Il., October 27-31, 2014. Santa Monica, CA: Human Factors and Ergonomics Society.

Simon, H.A. (1980). Cognitive science: The newest science of the artificial. *Cognitive Science, 4,* 33-46.

Uzzi, B., & Spiro, J. (2005). Collaboration and creativity: The small world problem. *American Journal of Sociology, 111*, 447-504.

Van Wijk, R., Jansen, J.J.P., & Lyles, M.A. (2008). Inter- and intra-organizational knowledge transfer: A meta-analytic review and assessment of its antecedents and consequences. *Journal of Management Studies, 45,* 830-853.

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

Zins, C. (2007). Conceptual approaches for defining data, information and knowledge. *Journal of the American Society for Information Science and Technology, 58(4),* 479-493.

TOWARDS USING THE FUNCTIONAL RESONANCE ANALYSIS METHOD TO BALANCE RESILIENCE AND ADAPTABILITY – A CASE STUDY OF MIGRATING A SOFTWARE PRODUCT INTO THE CLOUD

Marc Werfs
University of St Andrews, School of Computer Science, St Andrews, UK
mw62@st-andrews.ac.uk

Abstract

Cloud computing provides computing resources over the Internet. It has not only advantages such as cost savings but also introduces companies to new risks, e.g. less control over the infrastructure. These risks require companies to become more resilient while increasing their adaptability. To increase the resilience and adaptability, companies need to have complementary organisational changes when adopting cloud computing. Organisational changes are, however, difficult to carry out as explained by the envisioned world problem. By using the Functional Resonance Analysis Method (FRAM) this paper describes how a software vendor migrated one of their software products into the cloud. Two FRAMs were created, one before the migration and one after it, to show which organisational functions were changed in order to accommodate the new technology and wich remained unchanged in order to retain organisational elements employees and customers value. By finding this balance the software vendor was able to use the move to the cloud to become more resilient while increasing their adaptability.

1 INTRODUCTION

Cloud computing is a combination of technologies to provide remotely hosted computing resources. Next to offering many opportunities to software vendors, such as enabling them save costs by outsourcing infrastructure, it also introduces them to new kinds of risks. On the one hand, software vendors take over responsibilities previously held by the customer. Before the cloud, customers would install the software vendor's product in their own data centre and be responsible for it. In the cloud, the product is hosted with the cloud provider and managed by the software vendor. On the other hand, software vendors outsource tasks to the cloud provider over which they have only a limited amount of control. In case the cloud provider's infrastructure fails, the software vendor can do nothing but wait until it is restored. Therefore, cloud computing requires software vendors, and companies generally, to become more resilient while increasing their adaptability in order to be prepared for these new kinds of risks.

Becoming more resilient and adaptable while adopting cloud computing, or any new technology, is challenging, which can be explained by the envisioned world problem. The envisioned world problem states that it is difficult to anticipate the effects of technological change (Woods & Dekker, 2000). In other words, companies do not always know beforehand what organisational changes need to be carried out in order to adopt a new technology successfully. This paper suggests decomposing the envisioned world problem into two categories in order to provide a more structured investigation. The first category, *use uncertainty,* captures the fact that companies increasingly struggle to predict how new software products and technologies will be used because the market evolves more rapidly. People expect to use the latest technologies because they also use them in other areas, e.g. at home (Bughin, 2012) and some of these technologies can be used without the company knowing about them or having feasible ways of controlling the use, e.g. smartphones (Baxter et al., 2012, Manyika et al., 2013). The second category, *technology uncertainty,* captures the fact that technologies, like cloud computing, take away control from companies and give it to a third party over which they have only a limited amount of control. Companies also rely more on bigger and more connected systems (or systems of systems) that are vulnerable to unforeseeable and cascading failure events, e.g. when Amazon's cloud is having an outage it becomes headline news (Northrop et al., 2006).

This paper proposes to use the Functional Resonance Analysis Method (FRAM) to investigate the effects companies experience by use and technology uncertainty during the adoption of a new technology. Furthermore, this paper argues that companies that are able to dampen the effects of use and technology uncertainty are in a better position to become more resilient while increasing their adaptability. The FRAM, although initially developed for risk assessments and accident investigations, is an ideal tool to investigate the impact of use and technology uncertainty on resilience and adaptability as the FRAM focuses on what a system does rather than how it is structured. In order for companies to become *more* resilient (as companies can only be more or less resilient but never be truly resilient) it has to be made an inherent part of everyone's daily activities. Thus, a higher level of resilience can only be achieved by what people do (where the structure of the system can only support them in doing it, Roberts, 1990). The same can be argued for adaptability.

This paper is structured as follows. The next section explains the implications of use and technology uncertainty on the resilience of companies to understand how they can react to and anticipate organisational changes. The third section describes the elements and steps of a FRAM analysis. The fourth and fifth section describe how the FRAM has been used to analyse organisational changes of a software vendor from the Oil & Gas industry that moved to the cloud. The final section concludes this paper to suggest further research.

2 INCREASING RESILIENCE AND ADAPTABILITY UNDER UNCERTAINTY

By combining ideas from Normal Accident Theory (NAT, Perrow, 1984), High Reliability Organisations (HRO, Roberts, 1990), and dependability (Laprie, 2008) resilience can be defined as the adjustment of a systems functioning to maintain its dependability during changing conditions (Werfs & Baxter, 2013). This definition stresses the close link between the notions of resilience and adaptability: the more resilient a company becomes, the more adaptable they are likely to be (it does not, however, work the other way around!). When companies ignore use and technology uncertainty or do not deal with the effects appropriately, they are likely to experience a negative impact on their resilience and adaptability, as explained in the following.

In the notion of resilience, successes *and* failures both stem from performance variability. Resilience has to be actively maintained over time by adapting: both reacting to change (through feedback loops) as well as anticipating change (through feedforward loops, Hollnagel et al., 2006). A failure can be evaded, for example, when people, systems or organisations are able to use the information, resources and time that is available to anticipate potential risks and make approximate adjustments to their behaviour (Hollnagel, 2009). It can, therefore, best be understood as something a person, system, or organisation does rather than something it has. In today's complex and dynamic environment the conditions of work (i.e. how a system operates) never completely match the way they were designed because it takes several years to implement a system; a time in which the environment and conditions continue to change (Hollnagel & Woods, 2005). People, therefore, play a vital role in maintaining resilience, because they are the ones who are flexible and adaptable by adjusting their behaviour to new information, resources or time constraints (properties that are often lacking in technological systems, Ignatiadis & Nandhakumar, 2007).

People, however, can sometimes become *brittle* in performing their jobs resulting in a decrease in resilience and adaptability. Rasmussen developed the idea that people go through three stages of skilfulness (1983). At the beginning, people perform their jobs on a *knowledge* basis. They face unfamiliar situations and need to analyse the environment, develop plans, and test them. Testing can be done by trial and error, for example. Once people get more familiar with situations, they move to *rule-based* behaviour. People have developed procedures, either through experience or adopted from other people. They are, however, still able to describe explicitly what they are doing. People are not able to describe what they are doing when they move to *skill-based* behaviour. At this stage they are able to perform their jobs in a more automated manner and without conscious attention (Rasmussen, 1983).

In less uncertain environments, rule- and skill-based behaviour is desirable. As risks can be clearly identified companies aim to address and control these as efficiently as possible e.g. by developing procedures. In uncertain environments, e.g. created through the use of cloud computing, rule- and skill-based behaviour are less helpful. In these situations, companies will want to aim for knowledge-based behaviour, as people will be required to constantly analyse the environment and adjust their behaviour according to new information. Problem solving skills like trial and error become more important so that companies are able to react to and anticipate new circumstances quickly and head off problems that appear at the horizon (e.g. when the cloud provider changes the services they offer or customers demand a new product feature).

Knowledge-based behaviour is also necessary for employees (and customers) to decide on an individual level how they need to adapt to the new technology and what organisational elements they would like to retain. Moving to the cloud can create a lot of uncertainty among employees and sometimes also customers. Employees, for example, are concerned with their skills and daily routines and if the new technology will affect these. The notion of socio-technical systems suggests that companies need to find a balance between adapting the organisation to the new technology and retaining organisational elements employees and customers value (Trist, 1981). Finding a balance can help companies decrease the impact they experience from use and technology uncertainty. For cloud computing, for example, companies need to listen to their employees and customers to understand what they expect from cloud computing (to reduce the impact of use uncertainty). Otherwise, companies run into the risk that employees and customers take their own actions and, for example, rent cloud services that have not been approved by the company. At the same time, companies need to adapt the organisation to react to the fact that they cannot influence what the cloud provider does and how often the cloud resources are changed or updated (to reduce the impact of technology uncertainty). The FRAM can assist companies in finding a balance between adapting and retaining organisational elements to successfully decrease the impact of use and technology uncertainty.

3 ELEMENTS AND STEPS OF A FRAM ANALYSIS

The FRAM is a systemic approach that builds on the notion of resilience (Hollnagel, 2012). Situations are analysed by identifying functions that are necessary for everyday activities. The *functions,* shown in FRAM as hexagons, are abstractions to capture work routines and related resources, tangible and intangible, e.g. people, material, information, etc. Every function has six aspects that connect functions with each other: **I**nput, **O**utput, **P**recondition, **C**ontrol, **R**esource, and **T**ime.

The first step in a FRAM analysis is the identification of functions that are of importance or interest (e.g. *Marketing* could be a function). It is often advantageous to concentrate on high-level functions at first and go into more detail in later stages of the analysis. It is not important which function is identified first. In a FRAM analysis there are not always clear start and end functions. Furthermore, the aspects of the functions ensure that all necessary functions are identified, regardless of the first function that is being identified.

Once an initial set of functions has been identified, they need to be described in more detail by defining (some of) their aspects. The *Input* is used or transformed by the function to produce the Output. The Input also starts a function. The *Output* is the result of what the function does. With the Output the function is completed. The *Preconditions* have to be true or verified in order for a function to start. The *Control* aspect regulates or supervises a function so that the desired (or planned) Output is produced. The *Resources* are consumed when the function is executed. The *Time aspect* captures the different ways in which time can affect a function. For example, a function may need to be carried out before, after, or in parallel to another function.

Functions need to have at least an Input or Output. Only the Output of a function can be connected to aspects of other functions, i.e. connecting Precondition with Control is not allowed. It is often useful not to describe all aspects of a function at first, as this can make the analysis complicated and it is easy to loose sight of the bigger picture. Background functions, for example, can be used instead to capture aspects of a system that are important but not the focus of the analysis. Background functions only have an Input *or* Output and can be considered a placeholder for future analyses (background functions are grey in FRAM).

Once all functions and aspects deemed appropriate have been described, the performance variability of the system is analysed. The way in which the analysis of performance variability is integrated into the FRAM is partly explained by its name. The method focuses on the analysis of functional resonance (hence the name Functional Resonance Analysis Method). Failures in today's systems emerge because the performance of functions vary (due to technological, human or organisational elements) and sometimes the variabilities reinforce each other causing the variability of one function to be higher than expected and making it fail (which means that the failed function produces the Output too late, not at all, or imprecise, Hollnagel, 2012).

4 ORGANISATIONAL CHANGES OF A SOFTAWRE VENDOR MOVING TO THE CLOUD

To understand how use and technology uncertainty affect a software vendor that migrates their software product into the cloud and hence how they affect the resilience and adaptability of a software vendor, a FRAM analysis has been carried out with a SME software vendor from the Oil & Gas industry. The software vendor, in the following referred to as project partner or PP, develops and distributes a high-value project management software product. The PP hopes to develop new competitive advantages by being in the cloud, expand into new international markets and enable customers to use the product more quickly.

The FRAM has been applied to the PP in two steps. First, a FRAM showing functions and aspects before moving to the cloud was created with the help of the Managing Director. Second, the created FRAM has been adapted to show the functions and aspects after the migration into the cloud (again with the help of the Managing Director). In addition, data from a 12-month multi-stage study with the PP was used, in which the PP was interviewed several times during the migration process (see Werfs et al., 2014). In the following the main functions and aspects of the before and after cloud migration FRAMs will be explained.

The *before cloud migration* FRAM is shown in Figure 1. The two background functions, *Create customer profile* and *Customer extends contract*, shown in grey, constitute the start and end functions of the FRAM. The function *Acquire customer* converts potential customers into actual customers. The Output of this function is the accepted proposal of the PP by the customer. In addition, the customer receives a list of requirements that describe what kind of hardware and access to databases the product needs in order to be installed in the customer's data centre. The function *Customer sets up product environment* is responsible for setting up the hardware and access to databases. This function is outside of the PP's control and the customer has the final responsibility. Only when this function is completed and the Output (*Customer's data centre is ready*) has been produced, can the next function *Consult customer* start (i.e. it is a Control aspect). The *Consult customer* function tailors the product to the specific needs of the customer (reflecting the customer's business processes). After the function has been completed, the customer is able to use the product. The two last remaining functions, *Service customer* and *Increase customer satisfaction*,

support the customer in their short and long term use of the product. *Service customer* deals with everyday problems users might encounter, e.g. a report is not produced as expected. *Increase customer satisfaction* tries to retain customers by convincing them to buy upgrades or new products. To achieve that goal, the function uses the customer history that is the Output of *Service customer* to know what issues the customer's users struggle with and what new features they might desire, for example.

Two functions in Figure 1 experienced performance variabilities before the migration to the cloud. *Customer sets up product environment* sometimes produces the Output too late because customers often fail to configure necessary hardware for the product in time. S*ervice customer* sometimes produces the Output imprecise because customers often fail to install updates properly or they do not install them at all.

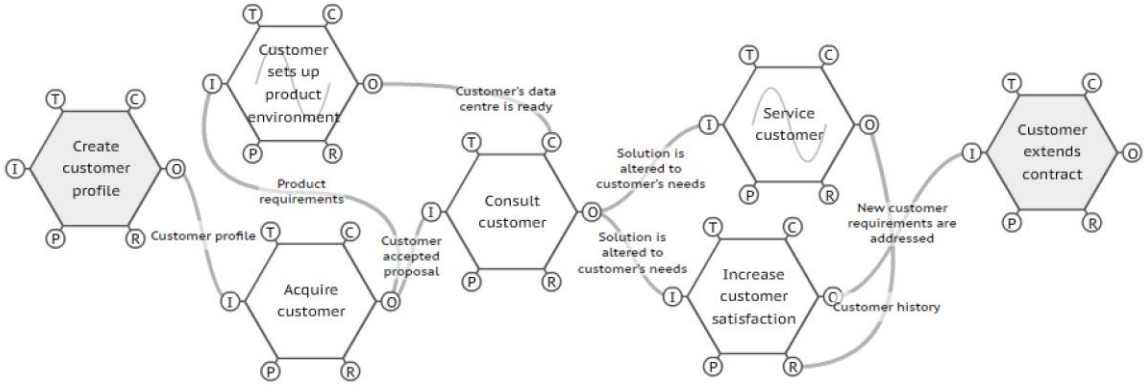


Figure 1. Before cloud migration FRAM: visualisation of the PP's functions and aspects before the cloud. The text boxes on the lines show the description of the aspects

By migrating the product into the cloud, two aspects of the relationship between the PP and their customers have changed. First, customers access the cloud-based product through a web-browser and do not have to install anything in their own data centre. Instead, the product is hosted with a cloud provider that provides the raw computing resources, such as servers, storage, network, on which the product runs and the PP manages the product installations of all customers. Second, because the product is now managed by the PP, the PP is also responsible for the uninterrupted operation of the product. Whereas previously, when the user of a customer encountered a problem they would contact their own IT department, they now contact the PP.

To reflect the changes in the relationship between the PP and their customers, the PP had to make several changes to functions and aspects (see Figure for the *after cloud migration* FRAM). The PP made some of the changes to address the previously identified performance variabilities. The performance variability in *Customer sets up product environment* could be eliminated as the function was replaced by *Initiate cloud environment*. *Initiate cloud environment* acquires the resources from the cloud provider (a task that can be automated and thus will only take a few minutes to complete for every customer). The performance variability in *Service customer* could be dampened by a move to the cloud as the PP is now responsible for installing updates. To do this appropriately and in a timely manner, the PP had to introduce two additional functions that service the product installations of all customers (1) in case updates need to be installed (function: *Upgrade customer solution*) or (2) customers experience problems with the product (function: *Maintain solution*).

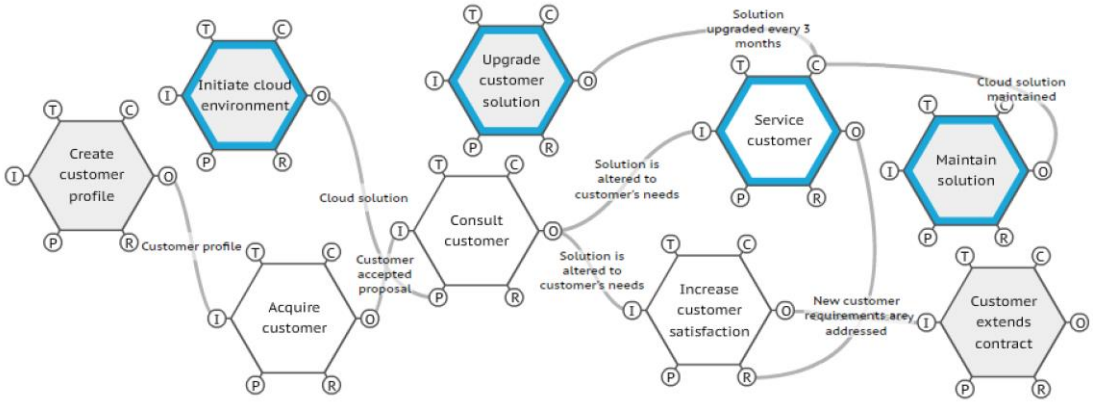


Figure 2. After cloud migration FRAM: visualisation of the PP's functions and aspects after the migration into the cloud. Functions that changed or have been newly introduced are highlighted by a blue frame

5 DISCUSSION

The Managing Director of the software vendor stated during the study that the goals for adopting cloud computing were clear. How to change the organisation to achieve the goals, however, was not clear at the beginning. Therefore, the software vendor adopted an ad-hoc approach in which they would only plan from step to step and adjust them based on new information, i.e. knowledge-based behaviour. The software vendor employed knowledge-based behaviour both on an organisational and individual level to (1) achieve a balance between adapting the organisation and retaining organisational elements employees and customers value and (2) to set the balance in a way that would dampen the effects of use and technology uncertainty, as explained in the following.

By comparing the before and after cloud migration FRAMs it is possible to understand how the software vendor found a balance between adapting to the new technology and retaining organisational elements employees and customers value. On the one hand, the software vendor wanted to exploit the advantages of cloud computing, i.e. offer the product to customers faster and increase customer satisfaction by managing the product for them. That is why the four functions highlighted in blue in Figure changed. On the other hand, the software vendor wanted to make the move to the cloud as efficient as possible to save time and resources. Furthermore, they wanted to be able to retreat from cloud computing in case adverse effects would have emerged. This strategy was necessary for the software vendor as they have only one core product from which they derive the majority of their revenue. If that product would fail in the cloud or customers would stop buying it, the software vendor would quickly experience financial difficulties. These are the main reasons why the software vendor kept two core functions unchanged: *Consult customer* and *Increase customer satisfaction.* By keeping these two core functions unchanged during the initial move into the cloud, the software vendor reduced the uncertainty employees and customers experienced during the migration to enhance the chances of adopting the new technology successfully. The software vendor might change these functions in the long-term to make them more appropriate for cloud computing.

The balance helped the software vendor in dampening the impact of use and technology uncertainty. In the cloud, the software vendor can monitor more closely how their products are being used. This allows them to dampen the impact of *use uncertainty* by reacting to and anticipating customer expectations and market demands quicker. The software vendor is able to see what functions of their products are being used and by whom, e.g. a manager or a technician. In that way, the software vendor can customise the product for different user roles, for example. In order to dampen the impact of *technology uncertainty* the software vendor had to find ways to work around the loss of control to the cloud provider. The software vendor reported that this can sometimes be an issue with customers as they are concerned with their data now being stored outside of their immediate control. The software vendor, however, managed to turn the implications of technology uncertainty into an advantage. In the cloud, it is easier to provide the product to customers and keep it up to date. This has increased overall customer satisfaction, although customers give away control over their infrastructure. Customers get the latest version of the product without having to do anything themselves. To further deal with the implications of technology uncertainty, the software vendor is working with a niche cloud provider, who is located close by and to whom they have direct contact. The software vendor knows, if something goes wrong, they can go directly to the provider and work with them (in contrast to bigger providers, like Amazon or Microsoft, where SMEs are more anonymous).

6 SUMMARY AND FUTURE WORK

Companies that adopt a new technology, like cloud computing, need to be aware of the effects of use and technology uncertainty. This paper suggested using FRAM to understand what functions are necessary to change in order to adopt the new technology successfully and what functions should remain unchanged because they are valued by employees and/or customers. The experience from the software vendor suggests that finding an appropriate balance helps companies in dealing with use and technology uncertainty to increase the company's resilience and adaptability. By doing before/after comparisons with FRAM, it was possible to assist the software vendor in deciding which functions should focus on resilience and which on adaptability: functions that provide the infrastructure for products need to be very resilient (e.g. *Initiate cloud environment*); functions developing new product features can be more adaptable to allow for the rapid prototyping of new ideas (e.g. *Upgrade customer solution*). FRAM also allowed the software vendor to understand the dependencies in the cloud: the customer relies on the software vendor for the operation of the product, which means that the more resilient the software vendor (and cloud provider) is, the more resilient are the software vendor's customers.

Building on the study presented in this paper, FRAM is currently modified further to help software vendors plan the organisational changes necessary to move to the cloud. The organisational changes are structured by the notion of capabilities. Capabilities combine resources, tangible and intangible, to achieve a specific task. The modified version

of FRAM will assist companies in understanding what capabilities currently exist in their organisation, if these will enhance or stifle a move to the cloud, and inform the development of new ones.

REFERENCES

Baxter, G., Rooksby, J., Wang, Y., & Khajeh-Hosseini, A. The ironies of automation: still going strong at 30? Proceedings of the 30th European Conference on Cognitive Ergonomics, ACM Press (2012), 65-71.

Bughin, J. (2012). Wiring the open-source enterprise. McKinsey Quarterly, (January), pp.1–4.

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

Hollnagel, E. (2012). FRAM: The Functional Resonance Analysis Method, Ashgate.

Hollnagel, E., Woods, D.D. & Levenson, N. (2006). Resilience Engineering: Concepts And Precepts, Ashgate.

Ignatiadis, I. & Nandhakumar, J. (2007). The impact of enterprise systems on organizational resilience. Journal of Information Technology, 22, pp.36–43.

Laprie, J.C. (2008). From Dependability to Resilience. In International Conference on Dependable Systems & Networks (DSN 2008). pp. G8–G9.

Manyika, J., Chui, M. & Bughin, J. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute, (May), p.163.

Northrop, L., Feiler, P., Gabriel, R., et al. (2006). Ultra-large-scale systems - The Software Challenge of the Future, Companion to the 21st ACM SIGPLAN conference on Object-oriented programming systems, languages, and applications - OOPSLA '06, p. 150.

Perrow, C. (1984). Normal Accidents, New York, NY, USA: Basic Books.

Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man, and Cybernetics, SMC-13, pp.257–266.

Roberts, K.H. (1990). Some Characteristics of One Type of High Reliability Organization. Organization Science, (1), pp.160–176.

Trist, E. (1981). The evolution of socio-technical systems - a conceptual framework and an action research program. In Conference on Organizational Design and Performance. p. 67.

Werfs, M. & Baxter, G. (2013). Towards resilient adaptive socio-technical systems. Proceedings of the 31st European Conference on Cognitive Ergonomics - ECCE ’13.

Werfs, M. et al., 2013. Migrating Software Products to the Cloud: An Adaptive STS Perspective. Journal of International Technology & Information Management, 22, pp.37–54.

Woods, D. & Dekker, S. (2000). Anticipating the effects of technological change: A new era of dynamics for human factors. Theoretical Issues in Ergonomics Science, 1, pp.272–282.

MANAGING RESILIENCE WITH A WEB OF KNOWLEDGE (WEKNOW) TO SENSE AND SHAPE COLLECTIVE STRESS SITUATIONS

Roberto Legaspi [1] and Hiroshi Maruyama [2]
[1] Research Organization of Information and Systems, Transdisciplinary Research Integration Center
The Institute of Statistical Mathematics, 10-3 Midori-cho, Tachikawa, Tokyo 190-8562, Japan
[1] legaspi.roberto@ism.ac.jp
[2] The Institute of Statistical Mathematics, 10-3 Midori-cho, Tachikawa, Tokyo 190-8562, Japan
[2] hm2@ism.ac.jp
http://systemsresilience.org/index-e.html

Abstract

We posit that our our models of systems resilience persistently demonstrate incomplete and fragmented knowledge bacause we fail to fully perceive the complexity of our systems and the collective stress situations (CSS) that perturb it. We argue for a framework to build a web of knowledge, or WeKnow, that embodies complexity absorption (integrated view of the laws of requite variety, knowledge, and complexity) and integrates data-centric, specialized and perceptual intelligence. WeKnow is aimed to provide a more holistic understanding of system structure, interaction behaviors, context, temporal and perceptual boundaries, emerging irregularities or inaccuracies, as well as proven or plausible alternative system resilience strategies. Ultimately, WeKnow is aimed to provide the capability to sense and shape impending, emerging, or ensuing CSS.

1 MOTIVATION

Despite the significant advances in science and technology, human and economic losses due to disasters, terrorist attacks, pandemics, social upheavals, and humanitarian crises remain significant. These situations, which can be referred to as *collective stress situations* (CSS), occur when due to internal or external shocks the system critically fails to provide the expected conditions of life to its components [Gillespie, 1988]. We believe that losses remain significant because we have yet to fully perceive the complexity of our systems and the CSS that perturb it. Their nature are indeed complex - nonlinear, spanning multiple simultaneous temporal and spatial scales, and with large interrelations and interdependencies among parts. Their evolving nature can affect physical, ecological, economic, and social dimensions simultaneously [Carpenter at al., 2009].

Our failure to fully perceive their complexity is because we tend to wrap our minds around the computable even though we are fully cognizant of the non-computable aspects of complex problems [Carpenter et al., 2009; Fowler & Fischer, 2010]. Another reason is that we heavily rely on the narrow, segregated, domain-dependent, and incomplete views of dominant experts rather than solving complex problems by engaging diverse perceptions [Carpenter et al., 2009]. Furthermore, we get intimidated in finding the critical links that mesh our human, environmental, social and technological systems into a cohesive and coherent whole. As a result, our models of systems resilience persistently demonstrate partial and fragmented knowledge.

Our proposed solution is a *web of knowledge*, or *WeKnow*, that embodies complexity absorption to account for the noncomputables and uncertainties associated with complexity. WeKnow is an integration of heterogeneous intelligence aimed to provide a more holistic understanding of system structure, interaction behaviors, context, temporal and perceptual boundaries, emerging irregularities or inaccuracies, as well as proven or plausible alternative system resilience strategies. Ultimately, WeKnow is aimed to provide the capability to sense and shape impending, emerging, on-going, or ensuing CSS. Sensing is the prelude to shaping that involves prediction, situation analysis and awareness, anticipation, as well as providing actionable information [Robertson & Olson, 2013]. Shaping is influencing and changing the course of CSS and the way the system responds adaptively.

2 LAWS OF REQUISITES AND THE THEORY OF COMPLEXITY ABSORPTION

Carpenter et al. [2009] suggest that to account for uncertainties, we must consider a wide variety of sources of knowledge, stimulate a diversity of models, and manage for the emergence of new syntheses that reorganize fragmentary knowledge. We further precise this by embodying in WeKNow three essential laws of requisites:

a. *Law of Requisite Variety*. By having diverse response and action mechanisms available to the system, the system is able to compensate a larger variety of perturbations [Ashby, 1958]. Richardson and Cilliers [2001] explained that the need for multiple approaches is to achieve a relative goodness of fit, i.e., since

knowledge can only be partial and fragmented, pluralism offers a venue to obtain the best possible elucidation of phenomena present in a given set of circumstances.

b. *Law of Requisite Knowledge*. Managing a perturbation is not only dependent on a requisite variety of actions in the system, the system must also know which action to select, and how, in response to the perturbation present [Heylighen, 1992]. Otherwise, the system would have to try out actions blindly and therefore compromise its survival.

c. *Law of Requisite Complexity*. The complexity of the system must be commensurate to the complexity of the environment in which it is embedded in order to function effectively [Boisot, 2003]. Casti [2012] theorizes that a system collapses due to the widening complexity gap between itself and its environment. To achieve requisite complexity requires complex adaptive systems capability of knowledge capture, creation and refinement [Gilpin & Murphy, 2008].

From the above, we can see that the laws are connected in that the first is incorporated in the second and the third incorporates both of the previous. We can also view this integration in terms of the theory of complexity absorption as explained by Gilpin & Murphy [2008]: In the multiplicity of options and diverse representations, albeit possibly conflicting, there is the ability to adapt and self-organize, as novel knowledge is obtained, or generated in order to modify an existing goal or adopt a new goal. Achieving complexity absorption (an integration of the three laws) leads to overcoming the partial and fragmented knowledge problem.

3 WeKnow FRAMEWORK

We now elucidate our framework for constructing WeKNow that embodies complexity absorption. Our framework involves multiple levels and dimensions that start with acquiring heterogeneous data from multiple sources that need to be fused and translated into the knowledge that will characterize a complex system capable of sensing and shaping CSS. We start with *how* knowledge is formed, and then *what* knowledge is derived and concluded from evidence using automated reasoning (i.e., inferred), and *to what* end.

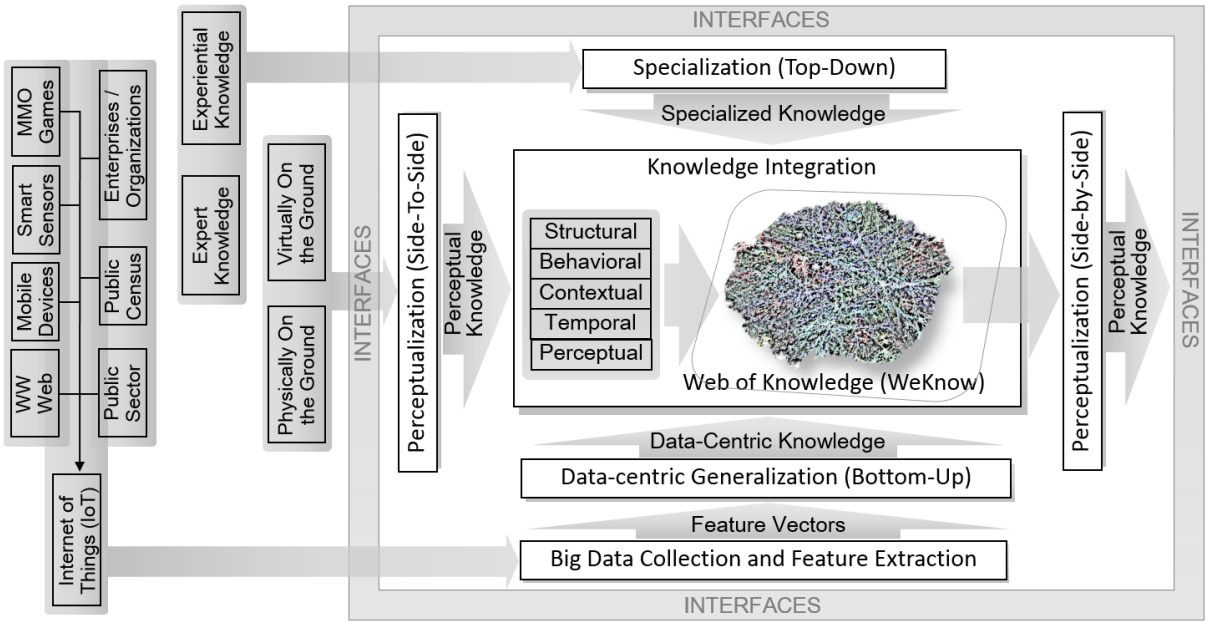


Figure 1. WeKNow framework

3.1 WeKnow HOW?

We are surrounded by information of incomprehensible and unimaginable amount. Information related to humans, enterprises, environments, and technologies, and their interactions are often reported from a multiplicity of sources, each varying in representation, granularity, objective and scope. Our human mind can only take in, let alone piece together, a portion of these vast amount of information usually on a need-to-know basis. However, with our advanced technological systems, we can do significantly much more, i.e., even to derive previously unknown meaningful information (knowledge) from raw data. Our framework espouses a socio-technical complex system with a three-pronged approach to deriving knowledge. Although numerous frameworks have the first aspect [Mitchell, 2012][Hall & Jordan, 2010][Mitchell, 2010][Liggins et al., 2009][Roy, 2001], they do not include the other two aspects of our framework.

3.1.1 Data-centric Generalization – A bottom-up approach

This universe is ever expanding as millions of data points are created every second form various sources. The Web is an open world and quintessential platform for us to share and receive information of various kinds. Our mobile devices have powerful sensing and computing capabilities that allow us to log our daily activities, do web searches and online transactions, and interact on social media platforms and micro-blogging sites, among others. Ubiquitous and interacting ambient sensors [Bohn et al., 2005; Poslad, 2009] can gather large volumes of human (e.g., mass movements, traffic patterns) and environmental (e.g., climate and weather changes, changing landscapes and their topographies, light and CO_2 emissions) data. There are massively multiplayer online games (MMOGs) that have become unprecedented tools to create theories and models of individual and group social and behavioral dynamics [Shim et al., 2011]. There are data that the public sector produces, which include geographical information, statistics, environmental data, power and energy grids, health and education, water and sanitation, and transport. There are the systematically acquired and recorded census data about households and the services (e.g., health and medical, education, water, grabage/waste disposal, electricity, evacuation, and daily living-related programs) made avaible to them. Enterprises (corporations, small businesses, non-profit institutions, government bodies, and possibly all kinds of organizations) may collect billions of real-time data points about products, resources, services, and their stakeholders, which can be insightful on collective perceptions and behaviours and resource and service utilizations. And lastly, there is the Internet of Things (IoT) that extends internet connectivity beyond desktop and mobile computers to a diverse range of devices that communicate and interact with the external environment - all via the Internet.

Data acquired from various sources tend to be heterogeneous in terms of their spatial and temporal aspects, data collection modalities, structure type (structured, semi-structured or unstructured), data type (hard physical data vs. soft data), and in sensor outputs with different resolutions and sampling rates. This data-centric approach should therefore consist of techniques and algorithms to preprocess the data to prepare them for the subsequent processes. The result of preprocessing will be a single concatenated feature vector that represents the set of features of the entities of interest (EoI), which can be objects or events that are endogenous or exogenous to the system. This is certainly a non-trivial task. If the varied data are commensurate, then raw signal data can be easily combined (e.g., using Kalman filtering). Otherwise, extracting a common feature vector may involve further data transformation, such as filtering out noises and outliers, data alignment (remove any positional or sensing geometry and timing effects from the various data), common referencing (obtain a common spatio-temporal reference), and data association (determine which object is associated to which event) [Roy, 2001]. Metadata may also be generated to describe the heterogeneous data [Hall & Jordan, 2010].

After the EoI vector is extracted, general models of the EoI should then be constructed. This is basically the kind of problem being addressed by data mining, machine learning, artificial intelligence, pattern recognition, time-series analyses, and many other methods.

3.1.2 Specialization – A top-down approach

Carpenter et al. [2009] suggest that the tendency to ignore the noncomputable aspects can be countered by considering a wide range of perspectives and encouraging transparency with regard to conflicting viewpoints. Our society puts more value in the dominant models, i.e., the ones we consider best practices because they are prescribed by experts, albeit there are evidences where the perceptions of “non-experts” (only because they lack formal education) but experience-filled individuals led to breakthroughs. Carpenter et al. [2009], for example, noted several cases: crucial information provided by village hunters and loggers prompted new approaches that saved the giant jumping rat in Madagascar from their sudden demise, and opinions and knowledge of indigenous fishermen saved endangered bumphead parrotfish.

Complex problems may have many solutions which may differ in the required execution to obtain the quality of the desired outcome [Carpenter et al., 2009]. Hence, a diverse team of experienced individuals is more suited than a team of expert solvers [Page, 2007]. Knowledge engineering approaches can be used to build and maintain knowledge-based systems that capture relevant contributions based on expertise and experience.

3.1.3 Perceptualization – A side-to-side approach

We use the term *perception* to refer to the process in which we *actively* and *purposefully* acquire, organize, and interpret the sensory information we receive in order to make sense of our environment and situation, as well as achieve environmental cognition, i.e., we structured our thinking on environmental circumstances and conditions (citations in [Legaspi et al., 2014]). The knowledge that are obtained in this approach are from individuals who are (*i*) *physically* on the ground, i.e., directly experiencing CSS, such as the members of the affected community, local government, law enforcers, first responders, and disaster managers, and (*ii*) *virtually* on it, i.e., are not in the affected area but have a good view of the CSS over the internet and in social media.

Here, social computing platforms, natural language processing, knowledge and ontology engineering, pattern recognition, and visualization can be used to gather, preprocess and organize the data, and infer perceptual knowledge that can function as feedback for situation analysis, awareness, and validation. However, at the other side of the framework, WeKnow's perceptual knowledge, i.e., information as perceived by WeKNow after it has integrated all knowledge, should be sent to the same individuals as actionable information for decision-making and response (hence, side-to-side). Here, the cognitive affordances of visual models can support the second perceptualization process. i.e., visualization can explicitly show the unified diverse knowledge in WeKnow.

3.1.4 Knowledge Integration and Incremental Learning

Once knowledge is inferred from these varied sources, the next step is to weave together these knowledge. *Knowledge integration* will involve inferring knowledge relationships among hugely varying domains into a coherent structure, while revealing hidden assumptions and reconciling areas of conflicts, inconsistencies, and uncertainties. It should describe how domain-specific concepts are interrelated for transdisciplinary problem and solution formulation. It must be able to synthesize micro-level, individualized and domain-dependent knowledge to contextual systemic knowledge. This task is difficult and remains to be an open research area.

Knowledge integration involves weaving the diverse knowledge into coherent networks, hence, a *web of knowledge*. Paperin et al. [2011] provide an excellent survey of previous works that demonstrated how complex systems are isomorphic to networks and how many complex properties emerge from network structure rather than from individual constituents. Representing the integrated knowledge into coherent networks can be accomplished by using network and dynamic graphs theories and models.

The specialized knowledge-based systems and the stored or incoming perceptual knowledge can be used to guide the data-centric generalization process as background knowledge (e.g., labels of objects and events for supervised and semi-supervised machine learning), feedback, and for validation. At the same time, any data-centric knowledge that was not accommodated in the other two can be used to correct or fine-tune their knowledge. Each can aid the others in pinpointing and correcting or clarifying malicious, erroneous, or conflicting information. Hence, the components of this tripartite knowledge elicitation can co-evolve together with increasing predictive isomorphism [McKelvey, 1999]. The inclusion of knowledge from diverse sources should not lead to vague generalities, but rather to become effective in completing our fragmented knowledge. Finally, new facts should be continuously derived and incoming evidence should be used to improve current knowledge repositories. Hence, WeKnow will be *learned incrementally*. The WeKNow framework, with its synergistic integration of knowledge, may enable an *emergent level of increasing intelligence* in the midst of complexity.

To conclude this subsection, the WeKnow framework therefore achieves *complexity absorption* [Gilpin & Murphy, 2009]: more than it integrates and preserves varied technologies for triangulating for the truth, it continuously tracks incoming and on-going information as well as evolving circumstances and conditions, and aids the system to better self-organize as it generates new information, infers new knowledge, adapts with new functions, and transforms to new goals. The objective of the framework is to unmask the heightened uncertainty created by the multiple sources of knowledge in order to be resilient in a complex world.

3.2 WeKnow WHAT?

We need to identify the properties that can be used to describe the complexity of the system, the CSS, and their interaction. We believe that the Five Aspects Taxonomy [Rhodes & Ross, 2009] ensures a good coverage of the essential aspects of the complexity we need to be knowledgeable of. The taxonomy is conceived for the engineering of socio-technical systems that exhibit complexities in multiple levels (components, subsystems, systems, and linked systems of systems) and dimensions (aspects).

The five aspects include: (a) s*tructural* - elaborate hierarchical/layered network arrangement of the components of the system, demonstrating couplings, interrelationships and interdependencies in multiple scales; (b) *behavioral* - variances in system responses to different stimuli; (c) *contextual* - environmental circumstances in which the system exists; (d) *temporal* - various system properties, dimensions and needs may change over time together with the dynamic environment in which it exists; and (e) *perceptual* - stakeholder perceptions of the system and its environment, which may change with context shifts and cognitive constraints and biases.

3.3 WeKnow TO WHAT END?

Given that WeKNow contains the connected and evolving knowledge derived from various sources about system and CSS structure, behaviour and context, and how they are perceived, to be changing over time, what then can we use the knowledge for? Again, for sensing and shaping of the EoI, which are most certainly the system failure and CSS that can threaten the existence of the system and its components.

Sensing can be achieved in a number of ways. By mining WeKnow, descriptive analysis can explain what has already happened and why it happened - after the fact or in real-time, and predictive analysis can forecast possible future outcomes across various scenarios or situations [Ernst & Young, 2014]. Second, after mining WeKNow for structures, behaviors, contexts and perceptions that are considered normal, routinary and expected, anomaly detection techniques can then be used to detect what is out of the normal, which can include proxy indicators or digital smoke signals of upcoming changes [Robertson & Olson, 2013]. Furthermore, while it is possible that conflicting information are received due to cognitive biases, perceptual errors, or communication differences, with various information coming from multiple angles, however, it is possible to perform multi-dimensional corrections and validations that can eliminate the false positives. Finally, there is potential for *unsaid analytics*, a term we introduce here to refer to inferring knowledge that was not explicitly stated because it depicts intuition, common sense, wisdom, and culture-based assumptions - those that are hard to quantify and measure but have proved essential to identifying anomalies and vulnerabilities.

The primary focus, however, is still is to provide actionable strategies that will convert sensing to shaping to avoid the worst consequences of CSS. Shaping via WeKnow can be achieved by prescriptive analysis to identify which decision and response will lead to the optimal or most effective result against a specific set of objectives and constraints [Ernst & Young, 2014]. Second, with knowledge about system interrelations and interdependencies, it is possible to implement creative chaos, i.e., to provoke sufficient perturbation to navigate the system into the portal of change. It is more efficient and effective to create situations that can force latent problems to surface than design the system to not fail, which, paradoxically, only makes it less resilient. By intriducing chaos into the system, not only do we make the system adaptive to failures, but we also let opportunities for innovation to surface since chaos would break tight couplings only to give way to new and previously unknown effective connections. Incidentally, the Five Aspect Taxonomy is claimed to be a basic frame to comprehend facets of innovation strategeis and communicate emeging technologies [Rhodes and Ross, 2009]. Third, we can use WeKnow to infer a lever point [Holland, 2005], i.e., the critical place within the system where applying a little change can make a big difference and a small shift a big change, and at that point the behaviour of the complex system changes fundamentally. We can also infer theories of system boundary, openness and modularity and their trade-offs [Carpenter et al., 2012]. Modularity can help contain ensuing CSS by compartmentalizing. However, too much compartmentalization can prevent aid from moving in and out of the system from various sources. Also, too much openness can casue harmful shocks to be transmitted or cascaded. Lastly, WeKnow can be used to provide real-time mapping of the events and feedback loops occurring during CSS. The ability to monitor the behaviours of human, environmental, social and technological systems in real time during CSS make it possible to understand where models, plans and policies are failing and to make adaptations.

4 CONCLUSION

On a complex systems point of view, we argued that the fundamental difficulty in managing resilience is the complexity that characterizes our system and the collective stress situations that result from perturbations. On an engineering point of view, we argued for managing resilience with an integrated knowledge of this complexity, which is automatically inferred from gathered, extracted, and structured heterogeneous intelligence about the nature and contextual interaction behaviours of our systems. With state-of-the-art technologies this integrated knowledge may learn incrementally and autocomplete itself. On a resilience point of view, we argue that with a holistic understanding of systems behaviour we can experience a paradigm shift in the way we view their vulnerability or resilience, hence, proactive. By sensing and shaping CSS, our systems become more adaptive. With this greater capacity to sense and shape, the system can better meet head-on the so-called unknown unknowns or uncertain uncertainties.

REFERENCES

Ashby,R.W.(1956). *An Introduction to Cybernetics*. London: Methuen.

Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F. & Rohs, M. (2005). Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. In W. Weber, J.M. Rabaey, and E. Aarts (Eds.), *Ambient Intelligence* (pp. 5-29). Springer Berlin Heidelberg.

Boisot, M. (2003). Is there a complexity beyond the reach of strategy? In E. Mitleton-Kelly (Ed.), *Complex Systems and Evolutionary Perspectives on Organisations: The Application of Complexity Theory to Organisations* (pp. 185–202). New York: Pergamon Press.

Carpenter, S. R., Folke, C. , Scheffer, M. & Westley, F. (2009). Resilience: Accounting for the noncomputable. *Ecology and Society* 14(1):13.

Carpenter, S.R., Arrow, K.J., Barrett, S. et al. (2012). General resilience to cope with extreme events. *Sustainability 4*, pp. 3248-3259.

Casti, J. (2012). *X-Events: The Collapse of Everything*. New, York, NY: HarperCollins Publishers.

Ernst & Young (2014). Big Data: Changing the way businesses compete and operate. *http:// www.ey.com/Publication/vwLUAssets/EY_-_Big_data:_changing_the_way_businesses_operate/$FILE/ EY-Insights-on-GRC-Big-data.pdf*, accessed on 04-05-2015.

Fowler, T. B. & Fischer, M. J., Eds. (2010). Rare events: Can we model the unforeseen? *Sigma 10(1)*, pp. 30-35.

Gillespie, D.F. (1988). Barton's theory of collective stress is a classic and worth testing. *International Journal of Mass Emergencies and Disaster 6(3)*, pp. 345-361.

Gilpin, D.R. & Murphy, P.J. (2008). *Crisis Management in a Complex World*. Oxford University Press, 2008.

Hall, D.L. & Jordan, J.M. (2010). *Human-Centered Information Fusion*. Norwood, MA: ARTECH House.

Heylighen, F. (1992). Principles of Systems and Cybernetics: An evolutionary perspective. In R. Trappl (Ed.) *Cybernetics and System '92* (pp. 3-10). World Science.

Holland, J.H. (2005). Studying complex adaptive systems. *Journal of Systems Science and Complexity 19(1)*, pp. 1-8.

Legaspi, R., Maruyama, H., Nararatwong, R. & Okada, H. (2014). Perception-based resilience: Accounting for the impact of human perception on resilience thinking. In *Proc. 2014 IEEE Fourth International Conference on Big Data and Cloud Computing* (pp. 547-554).

Liggins, M.E., Hall, D.L. & Llinas, J. (2009). *Handbook of Multisensor Data Fusion – Theory and Practice, Second Edition*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

McKelvey, B. (1999) Self-Organization, complexity, catastrophe, and microstate models at the edge of chaos. In Honor of Donald T. Campbell, J.A.C. Baum and B. McKelvey, (Eds.), *Variations in Organization Science* (pp. 279-307). Thousand Oaks, Calif: SAGE Publications.

Mitchell, H.B. (2010). *Multi-Sensor Data Fusion*. Springer-Verlag: Berlin Heidelberg.

Mitchell, H.B. (2012). *Data Fusion: Concepts and Ideas*. Springer-Verlag: Berlin Heidelberg.

Page, S. E. (2007). *The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies*. Princeton, NJ: Princeton University Press.

Paperin, G., Green, D.G. & Sadedin, S. (2011). Dual-phase evolution in complex adaptive systems. *Journal of The Royal Society Interface 8(58)*, pp. 609-629.

Poslad, S. (2009). *Ubiquitous Computing: Smart Devices, Environments and Interactions*. Wiley.

Rhodes, D.H. & Ross, A.M. (2010). Shaping socio-technical system innovation strategies using a Five Aspects Taxonomy. *http://seari.mit.edu/documents/preprints/RHODES_EUSEC10.pdf*, accessed on 04-05-2015.

Richardson, K.A. & Cilliers, P. (2001). What is complexity science? A view from different directions. *Emergence 3(1)*, pp. 5–22.

Robertson, A. & Olson, S. (2013). *Sensing and shaping emerging conflicts: Report of a Workshop by the National Academy of Engineering and United States Institute of Peace Roundtable on Technology, Science, and Peacebulding*. The National Academies Press.

Roy, J. (2001). From data fusion to situation analysis. In *Proc. 5th International Conference on Information Fusion*.

Shim, K.J., Pathak, N., Ahmad, M.A., DeLong, C., Borbora, Z., Mahapatra, A. & Srivastava, J. (2011). Analyzing human behaviour from multiplayer online game logs: A knowledge discovery approach. In H. Chen & Y. Zhang (Eds), *Trends and Discoveries 26(01),* pp. 85-89.

WHAT MAKE A COMPLEX SOCIO-TECHNICAL SYSTEMS BRITTLE: EVIDENCES FROM AN EVENT ANALYSIS

Luigi Macchi[1], Florence Magnin[1] and Jean Paries [1]
[1] Dédale S.A.S., 15, Place de la Nation, Paris, France
lmacchi@dedale.net

Abstract

A considerable operation was planned, prepared and executed in 2014 by the IT division of a major European corporation. The operation consisted in replacing two cores of the two data centres to simplify the architecture of the network, to improve its exploitation and to allow future technological evolutions. Despite months of preparation, several rehearsals in mock-ups, and despite trained, competent and experienced personnel, the replacement did not go as expected: part of the corporate network was slowed down, some communication lines were shut down, and back-up processes were disturbed. To cope with these problems, a crisis management unit was put in place and several days were needed before the IT division was able to return to its normal functioning. The relevance of the operation, the fact it was brought forward by the division management and the fact the solution of the problems required the participation of multiple actors contributed to make this event a major corporate crisis. An internal "accident" analysis was quickly performed by the IT division personnel. Four independent dysfunctions were spotted and a number of technical failures and human errors were identified as contributing factors to the event.

Unfortunately this event was not an isolate case. In the months preceding it, as well as in the following period, a number of other smaller unwanted events occurred. This situation shook both the team in charge of the operation and the whole IT division. It undermined the image of the division *vis-à-vis* of the clients, and the confidence they had in their ability and competences. The self-confidence of the IT division personnel was tackled as well. Overall, people's mind was deeply marked.

Despite the performed accident analyses the management of the IT division was still unsatisfied with the understanding of the "*deep*", root causes of the events. It was thus decided to take a closer look at the human and organisational factors which could have contributed to the "accident" and crisis. Since the internal accident analysis mainly focused on what happened during the operation, the management expressed the will to expand the analysis to the preparatory phase as well as to the crisis management one.

This paper presents the analysis process and the results of the investigation performed by the authors.

1 A WEAKENING CONTEXT

To understand the reasons behind the accident and to explain why few human errors led to a major organisational crisis, what happened during the planned operation has to be set in the overall organisational and operational context.

One of the leading objectives of the IT division is to improve and maximise its performance and to provide its clients (which are other divisions of the same corporation) the best and more effective technological solutions for their operational needs. This objective, coupled with the inherent tendency of the IT domain to look for and develop new technologies at a high pace, pushes the IT division to move towards a virtualisation and mutualisation of its services and products. The virtualisation of services, e.g. to move some services into *clouds,* and the mutualisation of products, i.e. to develop and implement shared IT products for the different clients, aims at reducing costs on facilities, power, cooling, hardware, administration and maintenance.

In conjunction with what can be considered a general trend of the IT industry, other contextual aspects deserve to be considered. First of all, the IT division is somehow subordinate to the other divisions of the corporation and it has to do its best to meet their expectations and respect the constraints they put forward. For the sake of the above mentioned mutualisation the IT division's operations tend to be more and more multi-clients (i.e. one operation concerns simultaneously multiple divisions of the corporation). In addition, since each client has different activities, the IT division has to deal with multiple specific, and sometimes conflicting, requirements. Finally the IT division has a recent record of multiple organisational changes including transfers and turnover of personnel (both at managerial and operational level).

All these aspects, as described in the results section of this paper, played a role in reducing the ability of the IT division to cope with the unexpected situation during the replacement of the cores of the two data centres.

2 UNDERSTANDING AN ACCIDENT BY UNDERSTANDING ORGANISATIONAL BRITTLENESS

A theoretical framework was needed to understand the reasons why a mayor crisis was triggered during the execution of the planned operation. This framework must provide a specific set of *lenses* to collect information and data, and to make sense of them. A first and traditional framework option would have consisted in looking into the technological failures and the 'human errors' which occurred during the replacing of the cores of the two data centres. To a certain extent this was the option taken by the IT division in preparing their internal accident report.

However, the fact that the IT division had been suffering recurrent incidents led to the presumption that this event was not an out-of-the-ordinary situation but rather the symptom of some dysfunctional mechanisms characterising the organisation. On the basis of this presumption, it was decided to adopt a systemic and resilience oriented perspective on the event investigation. This implied achieving a description of the event at the level of the socio-technical system as a whole, rather than looking only at local failures and errors. It also implied to understand the normal functioning of the IT division. Special attention was therefore placed on understanding the interactions between humans, technology, and organisation within the IT division as well as between the IT division and other relevant organizations and stakeholders.

Adopting this perspective the research question which steered the event investigation became: *What made the IT division so brittle that it was unable to anticipate and manage the unexpected events that happened during the operation of replacing the cores of its network?* And the analysis framework included two main concepts: the notion of *migration towards the boundaries of acceptable performance*; and the notion of *capacity of manoeuvre.*

The analysis of the event hence started with the acknowledgment of the natural tendency of organisations to migrate towards the boundaries of some kind of acceptable performance (Rasmussen, 1997) under pressures for achieving the objective of functioning *faster, better* and *cheaper*. By the very first interactions with the personnel (both at managerial and operational level) working in the IT division, it appeared evident that the organisation in question was not an exception to this general rule. By being pushed towards their functional boundaries, organisations are at risk of exhausting their ability of remaining in control of operations, i.e. to absorb disturbances and to stretch their functioning in case of sudden increase of demands. Woods and Branlat (2010) describe this ability as a *potential to gracefully extend* the functioning of an organisation over the boundaries of the acceptable performance. Such potential goes under the name of *Capacity of Manoeuvre (CfM)*.

The *CfM* of an organisation is influenced by two main factors. On one hand there is the way an organisation allocates its resources. Two main strategies are possible. The first one consists in striving for maximising performance efficiency in normal situations. This means that the organisation decides to reduce slack resources and buffers on the idea that, for normal operations, they represent unnecessary costs and excesses. The lean and total quality management perspectives are good examples of this management approach. The second one consists in allocating resources to cover for peak of demands and to deal with and overcome unexpected situations. It has to be pointed out how these resources will show they value only when disrupting events occur. The second factor influencing the *CfM* is related to the fact that an organisation exists and operates in a network of other organisations. Each of them, either intentionally or unintentionally, constrains or expands the *CfM* of the targeted organisation by their operational modes and by setting demands and requirements on the organisations they are related to. Despite the reasons behind the available *CfM* of an organisation at any given moment, it should be noted that the more an organisation is brittle the less it has capacity for adapting to surprises and this will require high amount of energy and resources.

3 DATA COLLECTION AND ANALYSIS

The event investigation was based on two main sources of information. The first one consisted in the review of the available documentation, i.e. the internal accident analysis report developed in the aftermath of the event as well as the minutes of the accident management meetings, an accident analysis report concerning another event which occurred a couple of months after the above mentioned one. The organisational structure of the IT division was as well part of the collected information. The second source of information consisted in the data collected during in-depth interviews and focus groups to gain knowledge about the three main phases of the operation i.e. its preparation (lasted almost a year), its execution and the crisis management. Sixteen in-depth interviews were conducted with:

- Representatives from the IT division directly involved in the event at both operational and managerial level.
- Representatives from client organisations (other divisions of the same corporation) which had been affected by the accident
- Representatives from the technical supply and support organisations

On the first round of interviews the topic discussed with the interviewees ranged from leadership and communication issues, to decision making and competence management, from professional culture to fatigue and working rhythms.

During a preliminary analysis of those data, some main topics were identified and a second round of data collection was organised. This was conducted in the form of two focus groups with a total of eleven representatives of the personnel from the IT division not directly involved in the accident. The scope of these focus groups was to understand the "normal" functioning of the IT division and explore the hypothesis that the human and organisational factors contributing to the event were not so unique and exceptional (as thought by the IT division management) but rather recurrent aspects of the overall organisational functioning.

The analysis was conducted by exploiting the theoretical framework to make sense of the information collected and to structure it in cluster of factors weakening the IT division and eroding its *CfM*. The preliminary results of the analysis were exposed and discussed in feedback meetings with the IT division personnel. This allowed to achieve a more solid and shared understanding of the reasons why the IT division was not able to anticipate the unexpected events that happened during the operation of replacing the cores of its network.

4 RESULTS OF THE EVENT ANALYSIS: WHAT MADE THE IT DIVISION BRITTLE

The reasons for the weakening of the IT division could be clustered in four layers ranging from a macro to a micro perspective. Each layer reduced the potential the organisation has to cope with unexpected situations and it contributed to the erosion of its *CfM*.

The four layers are:

1. Context and strategic choices (e.g. tendency of sharing applications for different clients)
2. Relationship between the IT division and the clients (e.g. submission of the IT division to clients' requirements)
3. Structural and organisational choices (e.g. lack of a precise methodology for managing changes)
4. Professional culture (e.g. step backwards perceived as a failure)

It can be considered that what happened during the replacement of the cores of the two data centres results from the normal ordinary functioning of the IT division rather than from some out-of-the-ordinary causes.

4.1 Context and Strategic Choices

The outer layer is related to the organisational context of the corporate and to the strategic choices made over the years**.** The choice to go for a mutualisation and virtualisation of IT applications has the drawback of making the technology so complex that it becomes virtually impossible for both managers and operators to fully know all the details of the technical system itself, of its functioning, and to identify all the risks which could be encountered in changing some parts of the system. As stated in one of the interviews: "*It is impossible to model everything. We run tests for the most of part of the functional aspects, and for what concerns the specificities we keep our fingers crossed*". The choice of mutualising applications among multiple clients has another effect: one problem impacts multiple stakeholders and a broader section of the network at the same time. Thus, when an incident occurs both the pressure to solve it and the perception of its criticality increase.

The effort to increase and optimise performance of the network pushes operators of the IT division to accept risks they would not accept under different conditions and contexts. This effect is amplified in those cases, as the operation of core replacing, where the projects are supported by the hierarchy of the organisation since operators perceive a higher pressure for accomplish their missions. Simultaneously to the aim of mutualising applications, the effort to optimise performance leads to the creation and deployment of more and more specific and dedicated applications to answer clients' needs. The proliferation of applications makes it challenging to assess and identify the sources of problems when they appear.

4.2 Relations between the IT Division and the Clients

The second layer comprehends the factors related to the relations of the IT division with respect to its clients and to the overall corporate.

Due to the fact that between the IT division and the other divisions of the corporate there is a supplier-client type of relation, the IT division is bound to satisfy the requirements and expectations of the clients and is subject to the pressures they put on it. This has been the case for the three phases (preparation, execution and crisis management) of each activity the IT division carries out. For example, during the preparation phase the IT division is limited by its clients in the selection of the time and planning for the operation. According to one of the interviewee "*[the clients] are always winners in the negotiation; finally there is not a real negotiation*". During the execution phase the IT division is pressured by the clients for respecting the planning of the operations. This pressure can sometimes be

implicit and "simply" perceived by the IT personnel as one of the interviewee expressed: "*We had already postponed the check 5 or 6 times, and we did not want to delay it once more*". Even in the case of a crisis management, the IT division is affected by the pressure of its clients. This is the case, for example, when a solution to a problem has to be found and different conflicting logics exist. While the IT personnel would prefer to address a crisis by thoroughly understanding the reasons behind a problem, the clients are keener in finding a quick fix to the issue. As in the case of the event here discussed, the strategy for coping with the crisis was to a certain extent decided by the clients. This fact was perceived by most of the IT operators as unfair and it exacerbated tensions and frustrations.

The relation with the other divisions of the corporate plays as well a role in the process for demanding the authorisation to execute the operations. Since the other divisions are often critical toward the execution of operations, the IT division has to spend time and effort in communicating with them about the upcoming operations and the risks associated to them. To facilitate the task of obtaining their approval, the IT division tends to minimise, in its communication, the impacts the operations could and would have on the core activities of the corporation. The drawback of doing so is that the IT division creates idealistic expectations on the way operations will go and on the complete absence of risks; as an interviewee reported: "*We anticipate their refusal so we include less information and we state the operation will have no impact at all*".

With respect to the relation between the IT division and the clients a third and final factor making the IT division brittle exists. In order to comply with the other divisions' stringent requirements in terms of the availability of their applications, the IT division is sometime pushed to trade safety for efficiency in the way to execute its operations. An illustrative example of this situation is that the IT division decided to change the cores of both its datacentres simultaneously rather than doing it in two times. The second option would have been more cautionary (at least they would have been sure that one of the datacentre was operative) but it would have implied that some clients would have been bothered two times and not just one.

4.3 Structural and Organisational Choices

The third layer contributing to make the IT division fragile in the face of unexpected situations comprehends multiple factors related to the structural and organisational choices. A first set of factors in this layer is related to the process and approach for conducting changes and performing operations. To make sure that all operations on the network are authorised by relevant stakeholders, the IT division put in place a dedicated organisational system. This system raises issues with respect to its effectiveness. Sometimes it is not the most appropriate representative of a client organisation who grants the authorisation and therefore some constraints can be not considered at this stage. In addition, a technical perspective on the operation is often lacking, and the organisational system does not allow a clear differentiation and identification between operations at high or low stake. Finally, by the fact that the documentation of the organisational system is normally compiled by highly specialised IT personnel and read by non-technical personnel, it is often prepared in a technical jargon difficult to be understood by the receivers.

The IT division does not impose on its personnel a strict methodology for preparing operations. For this reason there is a rather big variety in practices. This includes, for example, the way in which operations are classified (as an IT project with all the administrative aspects related to it, or not). As a side effect of this situation, there are uncertainties in the way operators allocate their time to preparing operations, in the way managers follow that preparation, in the way validation milestones are implemented, and in the way risk analysis is performed. These uncertainties are experienced by the personnel of the IT division which declared, for example, that "*Up to today, I still do not know if I should have been part of the management team of the project or not...*" or that "*[For that operation], we did a risk analysis by rule of thumb"*

Sometimes the IT division is pressured to perform multi-site operations (mainly to accommodate clients' constraints). As in the case of the accident occurred, this can complicate the construction of a shared understanding of what is going on at the sites. In addition, this increases the temporal pressure for synchronising operations and can lead (as it has been the case) to misunderstanding and incoherent decisions.

4.4 Professional Culture

The specific professional culture which could be observed at the IT division also played a role in making the socio-technical system fragile. The personnel is highly committed to their work. This positive and desirable trait has led in the past as well as during the execution of the operation of replacement of the data centres to some side effects. For most of them it is difficult to step back from an operation or an activity. It appears to be difficult to "*say no*" to challenges and work demands. The commitment of the personnel for example resulted in a problematic shifts' change during the event in analysis. Some operators did not want to leave the operation site because they wanted to help and know how things developed, as well as others did not respect the instruction to take a day off from work because they cared about the result of the work and "*wanted to know where they were"* with respect to the resolution of the problem.

For each operation the possibility to withdraw from its execution and the reestablishment of the main functionality of the system is considered. As a matter of fact the personnel, even when it prepares for it, does not really conceive the withdrawal as a realistic possibility. It is perceived as a failure and therefore it is postponed as much as possible. The withdrawal is often used as an argument with the clients for obtaining the authorisation to perform operations in the sense that "*in case of problems we can at any time withdraw and you [the clients] will not be affected*".

Another cultural trait characterising the IT division is the gap between the managerial and the operational level. This is evident in the different degree of technical knowledge the two groups have. Since it is typical of the IT domain a rapidly evolving technology, managers often possess an out-of-date technological competence which limits their possibility to follow up operations in their preparation and execution. Even in the case of incidents they have limited visibility on the technological problems, and their focus to solve an accident (i.e. to resolve it quickly) is different from the one shared by technicians (i.e. first understand the problem then fix it).

5 DISCUSSION AND CONCLUSION

The complexity of the work performed by the IT division and the level of uncertainties associated with it make it de facto impossible to foresee all the potential problems emerging during operations and prevent their occurrence. The analysis of the accident which occurred during the replacement of the cores of the data centres allows identifying a number of factors which contributed to erode the Capacity for Manoeuvre of the organisation. For the sake of presenting the results of this analysis, those aspects have been clustered in four main layers of weakening factors. The aspects and their effect on the IT division are summarised in the following table:

Table1. Summary of impacts on the brittleness of the IT division

Virtualisation	Increased difficulty to foresee barriers for identified risks Increased difficulty to adapt to hazards
Mutualisation	Increased possibility for problems to widely spread in the network Increased possibility for problems to affect multiple clients
Optimisation of performance	Increased risks acceptance for meeting performance demands Increased difficulty to assess the source of problems
Relation with clients	Reduced preparation time Increased time pressure which could lead to errors
Organisational system for authorising changes does not allow an optimal preparation of operations	Increased difficulty to assess and validate technological solutions
Difficulty to build a shared vision of the situations in case of multi-site operations	Increased possibility for misunderstandings and incoherent decisions
Management with out-of-date technical competences	Increased difficulty to follow operations' preparation and execution Increased difficulty to take over crisis management
Withdrawal from operations considered as a failure	Contingency plans insufficiently prepared
Commitment to work	Increased difficulty to hand over tasks execution
Multiple strategies for problem solving	Increased difficulty to build a shared strategy to solve problems

The traditional approaches for preventing human errors and addressing organisational factors seem to have reached their limits in supporting organisations to further improve safety level. The concepts of human and organisational reliability fall short in ensuring accidents prevention. The same appears to be true for the safety management approaches aiming at constraining performance and reducing internal and external variability. The Resilience Engineering community has been advocating for a change in safety management approaches and practices for more than a decade (e.g. Hollnagel, 2004; Hollnagel et al, 2006; Hollnagel et al, 2008; Dekker, 2011).

The framework exploited in this event analysis acknowledges that complex socio-technical systems operating in a network of organisations are pushed towards the borders of a space of acceptable performance by multiple

conflicting pressures. This approach offered a practical perspective for identifying, highlighting and acknowledging the elements which reduce the IT division's capability to effectively cope with surprises. The results of this analysis provide content for the management of the IT division to rethink their safety management approach and to evolve in their safety management practices. While the possibility to work and invest time and resources in improving operators' reliability and enhancing safety culture should not be neglected, it seems that this will not be enough for making the IT division less brittle. At least three lines of work could be conceived for expanding the *CfM* of the IT division - or at least for limiting its erosion. The first two concerns accidents prevention. One consists in conducting a reflection on the elements which make the system brittle i.e. by identifying and revealing the impacts of the strategic choices (e.g. mutualisation of applications) on the activities of the IT division. The other consists in reducing the possibility for vagaries. In the specific case of the IT division this would mean for example to define, in collaboration with the clients, a set of maintenance slots during which operations could take place. This would have the effect of facilitating the obtaining of authorisation for operations, of easing the communication about risks and of reducing the tensions between the IT division and its clients. Finally, the third line of work concerns how to deal with and recover from unexpected events. Improving risk understanding (for example by classifying operations according to their sensitivity) and accident management (for example by creating buffers in the system to reduce the impact of accident) represent a possible strategy for expanding the capacity for manoeuvre of the organisation.

REFERENCES

Dekker, S.W.A., 2011. Drift into Failure: From Hunting Broken Components to Understanding Complex Systems. Ashgate Publishing Co., Farnham, UK.

Hollnagel, E. (2004). Barriers and accident prevention. Aldershot, UK: Ashgate.

Hollnagel, E., Woods, D. and Leveson, N. (Eds.). 2006. Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate

Hollnagel, E., Nemeth, C. P. & Dekker, S. W. A. (Eds.) (2008). Resilience Engineering Perspectives, Volume 1: Remaining Sensitive to the Possibility of Failure. Aldershot, UK: Ashgate.

Rasmussen, J. (1997): Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, 27(2/3):183-213.

Woods, D. D., & Branlat, M. (2010a). Basic Patterns in How Adaptive Systems Fail. In E. Hollnagel, J. Pariès, D. D. Woods & J. Wreathall (Eds.), Resilience Engineering in Practice (pp. 127-144). Farnham, UK: Ashgate.

CLOSURE

PAPERS POSTER SESSION AND WORKSHOP

The chapter PAPERS POSTER SESSION AND WORKSHOP summarizes contributions in workshop and poster sessions, not all contributions were available in print unfortunately so the overview is not complete. The workshop and poster presented were selected by the Programming and Scientific Committee.

The workshops were programmed on Monday 22nd June while the poster session was continuous from 23rd-25th June 2015. The poster presenters got the floor in the plenary program to pitch their poster.

Training for operational resilience capabilities in an organizationally coherent manner (workshop)

Johan van der Vorm [1], Tor Olav Grøtan[2] and Luigi Macchi[3]
[1] Netherlands Organisation of Applied Research, TNO
Leiden, Netherlands
johan.vandervorm@tno.nl; +31621134472
[2] SINTEF Technology and Society, Trondheim, Norway
tor.o.grotan@sintef.no
[3]Dédale, Paris, France
LMACCHI@dedale.net

Workshop abstract

The development of methods for resilient operations is sought to facilitate companies to develop adaptive practices is a quest many are busy with. Resilience sometimes faces its borders when compliance policy of companies comes into the forefront. But when compliance framework is dominant, what adaptive practices teams do and are able develop and what can be learned from it to improve resilient capabilities?

SINTEF, Dédale and TNO are cooperating with several companies ENI (NO); Strukton Rail, NAM and Infraspeed Maintenance BV (NL) to develop a program for training operational capabilities. This project team on Training operational capabilities (TORC) proposes to share the knowledge and exchange experience with the symposium participants and to explore relevant resilience capabilities.

The goal of the workshop is to let participants get a better insight in and letting them experience what resilient capabilities are. But also to explore how companies can train for them in order to improve adaptability without falling into adaptive traps and blame-games. An important goal is to address the relation between operational capabilities and managerial capabilities, and how these capabilities can be trained in a joint and coherent manner.

The question will be discussed how much space of manoeuvre in business operations is available for individuals and teams and what is the influence of a compliancy context on resilient behaviour? Employees and managers each need to develop strategies for anticipation and cooperation for adaptive responses to variation and surprises in everyday business. What do employees and managers need to be able to adapt successfully and to prevent to fall in an “adaptive trap”. Training operational capabilities needs to engage both sharp and blunt end.

A tentative program is:

1. Introduction
    a. What are resilient capabilities?
    b. Why do you need them, how can you maximize the yield without increasing risk in an organizationally coherent manner?
    c. What dynamics are involved?
2. Some exercises around industry cases presenting specific situations challenging people (operational, managerial, joint/integrated) to determine what adaptive behaviour is necessary.
3. Discuss what adequate resilient response is.
4. Reflection:
    a. What do we consider as crucial resilient capabilities?
    b. How can we improve them by training?
    c. Examples from practices of people

For resilience in business operations like in rail, oil&gas, "sharp end" people need to be capable to monitor, anticipate, respond and learn. Adaptive behaviour will result from resources available in individuals, teams and organisation, and has a pronounced "situated" or "bottom-up" character in which the necessary margins of manoeuvre are experienced. However, without managerial supervision and guidance, constituting a legitimate space of manoeuvre, the probability of adaptive failure, but also lack of clear accountabilities and responsibilities, becomes imminent. Effective operational behaviour will be successful when people are aware of their situation,

know how to decide and act and reflect on it. Communication is essential.

Training is a way to improve capabilities of individual team members, the team itself and, not at least, managerial support. Their cooperation is essential in deploying necessary resources and orchestrating adaptive courses of action with sufficient organizational and managerial rationale and intent.

SCALES10 AS A PRACTICAL TOOL TO SUPPORT MONITORING OF THE SYSTEM FROM DIFFERENT VIEWPOINTS

Ivonne Herrera SINTEF, Norway
Martina Ragosta, Deep Blue, Italy

Workshop abstract

By active involvement participants will identify and discuss potential use of resilience related indicators. From analytical and small group work, participants are invited to use SCALES framework and its associated tool and have hands-on experience on practical cases of everyday operations.

Safety is not seen as a competition with the core productivity business. On the contrary, safety is seen as an integrated part of the production processes. SCALES combines knowledge from Resilience Engineering and Enterprise Architecture (EA) integrating and modelling human, organizational and technical aspects, dependencies within and across organizations. Thanks to the EA, different perspectives are explored through dedicated viewpoints. SCALES includes a functional viewpoint, a process viewpoint and an information viewpoint. In addition, we are proposing a new viewpoint, the Resilience viewpoint aiming to identify, explore and modeling a set of indicators from the former views as patterns. Indicators are not isolated but affect each other influenced by the context of operations.

An important aspect of the Resilience Engineering agenda is the development of practical approaches that enable systems/organizations to continue operations when facing expected and unexpected changes, opportunities and disturbances. This workshop focuses on a practical tool based on enterprise architecture for modelling and analyzing resilience concepts. These are presented in patterns consisting of practical interrelated indicators. This tool is not confidential and is available for members outside SCALES consortium and will be provided to wider research and industry community. Current version of the tool is adapted to Air Traffic Management by participating in the workshop. Participants will be able to explore and evaluate which aspects can be adapted to other safety critical domains.

The facilitators introduce SCALES framework, associated tool and workshop. Participants will be asked to work in small teams to explore in an interactive manner and discover SCALES. By the end of the session instead of a person taking notes, we will ask a “visiting expert” (participants) from each team to share lessons learned with the focus on using SCALES in their practical world.

Acknowledgement – Disclaimer

This work is co-financed by EUROCONTROL acting on behalf of the SESAR Joint Undertaking (the SJU) and the EUROPEAN UNION as part of Work Package E in the SESAR Program. Opinions expressed in this work reflect the authors' views only and EUROCONTROL and/or the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

[10] SCALES is acronym of SESAR WP-E project: Resilience potential and early warnings for Air Traffic Management in case of system degradation through Enterprise Architecture

SOCIO-TECHNICAL SYSTEMS, ADAPTION AND VARIABILITY – AN INTRODUCTION TO THE FUNCTIONAL RESONANCE ANALYSIS METHOD (workshop)

Gesa Praetorius 1 and Milena Studic 2
1 World Maritime University, PO Box 500 SE-20124 Malmö, Sweden
1 gp@wmu.se ; +46(0) 40356 374
2 Imperial College London, South Kensington Campus, London SW7 2AZ, United Kingdom
2 m.studic11@imperial.ac.uk

Workshop abstract

The Functional Resonance Analysis Method (FRAM) is a method to functionally model complex socio-technical system (Hollnagel, 2012; Hollnagel, 2014). A large body of research indicates this method's significance to understand how socio-technical systems operate under normal and abnormal conditions, and it has widely been used to analyse the accidents and incidents in high hazardous domains such as the aviation (Woltjer & Hollnagel, 2007) and the maritime domain (Praetorius, Lundh, & Lützhöft, 2011).

Today's socio-technical systems are complex and act in uncertain and dynamic environments, where functions are distributed over people, technology and organisations. Systems need to adjust their performance to be able to cope with the complexity of daily operations and meet current demands arising from the context. As these adjustments are based on the availability of resources (e.g. time, manpower) they will always be approximate. Consequently, everyday performance is and needs to be variable to help the system successfully adapt its functioning to the current operational conditions. The FRAM offers a way to identify and analyse system adjustments in terms of functional units and their interactions within variable demands of everyday operation.

This tutorial offers an introduction into the FRAM and its various applications. FRAM analysis will be demonstrated on examples from the maritime and aviation domain in a step-by-step fashion. Furthermore, methods to collect data and inform the system modelling are presented and discussed to highlight the challenges and opportunities of the FRAM for risk and resilience assessment.

The FRAM represents one of the few most established methods for a resilience assessment. A tutorial presenting the method can trigger interesting ideas and discussions regarding how to use the FRAM to monitor and manage performance variability and therefore also identify ways in which a system's resilience can be maintained and possibly strengthened.

RESILIENCE IN ACTION – WHEN TO INVEST TO BECOME MORE RESILIENT? (workshop)

Ivonne Herrera SINTEF, Norway; Jörg Lenhardt DFS, Germany; Rogier Woltjer LiU/FOI, Sweden; Tom Laursen IFATCA, Denmark; David Woods OSU, USA; Anthony Smoker IFATCA, UK, Tony Licu, EUROCONTROL, Belgium.

Workshop abstract

Enable participants to imagine a future where systems/organizations operate in a resilient manner both in regards to design and operations. Specific stories, practical examples, and resilience topics will be presented to the participants. Example of stories:

- Everyday successful operations to investigate how adaptive systems work, to achieve a better understanding the operational capability in terms of abilities to monitor, anticipate and respond;
- Extreme situations where demands increase to explore the ability to sustain operations and its capacity of maneuver;
- Introduction of new technologies and automation surprises to investigate benefits and new vulnerabilities.

Resilience principles and topics will, amongst others, cover leading indicators, early warnings, weak signals, managing trade-offs (e.g. efficiency-thoroughness, flexibility-stiffness); cross-scale interactions (how systems/organizations can be well adapted locally, but maladapted globally). The participants will be asked to explore topics related to different degrees of performance and resilience. The tasks aim to explore and discover ways to enhance resilience. This is expected to be a joining activity between practitioners from the industry and academia.

An important aspect of resilience is its support to business continuity and the ability to continue operations. The idea is to use innovation games as an integral part of the RE research agenda. These games facilitate interaction and creation of solutions that are relevant to the domains involved in the development of knowledge and practical tools.

LOSS OF CONTROL: AN INHERENT FRONTIER FOR MANAGING RESILIENCE? (workshop)

John Stoop1 and Jan de Kroes1
1Kindunos Safety Consultancy Ltd
Spijksedijk 8, 4207GN Gorinchem, the Netherlands
stoop@kindunos.nl

Workshop abstract

The contribution highlights one of the most challenging discussions on whether or not a proactive approach in complex, open and dynamic systems is possible. If pro-action is not possible, only a reactive approach remains, leaving researchers to investigating emergent properties in practice. Loss of control in aviation can be considered an inherent property if analysed simultaneously along lines of design, control and practice. Analysis from a systems perspective reveals the actual, factual, critical and potential change triggers, agents and drivers which enable sustainable intervention, dealing with the inherent characteristics of the system at all control levels. The contribution clarifies challenges in the translation across disciplines and life cycle phases as well as the transition from an event factor approach to a system vector approach. Such a transition makes the concept of resilience accessible for designers and change agents and strengthens the credibility of the notion of resilience. Selection of the Loss of Control function in aviation also indicates that a failsafe system is not likely to exist at the level of socio-technical and socio-organisational systems due to their characteristics as an open, global network configuration with delegated and distributed responsibilities. Reconsiderations at the level of notions and paradigms seem inevitable.

1 INTRODUCTION

This contribution elaborates on the development of devices that are designed to control an inherent risk of flying with potentially catastrophic consequences: stall. The tragedy with AF447 and several subsequent events have served as a wakeup call for the aviation industry to deal with a type of accident that had disappeared from the agenda. A combination of automation applications and envelope protection seemed to have tackled the phenomenon to an acceptable low level of occurrence. Based on these triggering events, multiple analyses into the causes of upset recovery have been performed, suggesting a variety of remedies to tackle the issue. Many of these solutions focus on conventional engineering, education or enforcement strategies, assuming a one to one relation between cause and solution. These strategies have reduced the stall phenomenon to an acceptable low frequency event with a high recovery potential. However, stall is a phenomenon in a highly complex and dynamic operating environment in a socio-technical systems context. Such a phenomenon can only be perceived from a combined scientific, technological and societal perspective. Exploring the potential of adaptivity and resilience engineering has revealed new solutions, covering several patents and innovations. Ultimately, this approach has materialized in a preliminary design of a water bomber aircraft.

From the early days of aviation, stall has been an inherent hazard. Otto Lilienthal crashed and perished in 1896 as a result of stall. Wilbur Wright encountered stall in 1901, flying his second glider. Stall is a condition in which the flow over the main wing separates at high angles of attack, reducing the airplanes capacity to gain lift from the wings. Stall only depends on the angle of attack, not on airspeed. Airspeed is used as an indirect indicator for approaching stall conditions. Stall speed varies depending on weight, altitude, and configuration. Many devices have been developed to postpone stall, reduce its severity or to improve recovery. Any yaw of the aircraft entering stall may result in autorotation, that may develop into an almost irrecoverable ‘flat spin’. Stall recovery is possible by training appropriate manoeuvres as a part of basic flying skills. If applied correctly, a nose down position and increasing power until smooth air flow over the wing is restored leads to a small loss in altitude. Some fixed wing aircraft configurations are more susceptible to stall because turbulent airflow may blanket control surfaces at the tail. At low altitude the dangerous aspect of stall is a lack of altitude for recovery. At high altitude, the small margins between minimal and maximum airspeed are referred to as the ‘coffin corner’. In contrast with most military aircraft, civil aircraft do not have excessive power to thrust vector an aircraft through the stall flight region.

During low speed conditions, aircraft are sensitive to stall due to the ratio between drag and power. This flight condition is caused by the fact that induced drag is a by-product of the generated lift. At high angles of attack the lift vector contains a considerable rearward component, increasing the induced drag with increasing angle of attack.

Such drag cannot be compensated by steadily increasing power, which creates flying in a condition 'behind the power line'. A specific form of stall occurs when the aircraft makes steep turns with a load factor higher than 1g.

Over the decades, a wide variety of conventional stall warning and protection systems have been developed, categorized as aerodynamic devices, mechanical control devices or warning devices. Modern civil aircraft are protected against stall by flight envelope protections which limit their manoeuvrability. Specific sophisticated class of stall devices are 'canard' wings and fly by wire Flight Control Mode systems to cope with aerodynamic instability inherent to a positive lateral moment coefficient. Specific training simulators and programs have been developed for high altitude upset recovery. Each of these devices focus on a specific contributing factor in the event sequence. Stall is a specific aerodynamic phenomenon and part of a more generic failure mode, which is inherent to aviation: Loss of Control.

2 LOSS OF CONTROL

Loss of control (LOC) is the leading explanation for fatal accidents in several segments of the aviation industry, each with specific fleet composition characteristics (Veillette 2012). Several major events in large commercial aviation indicates deficient pilot knowledge and piloting skills, resulting in a lack of pilot resilience, leading to fatal loss of control accidents (West Carribean Airways 708, Air France 447, Colgan Air 3407, Turkish Airlines 1951, Asiana Airlines 214 and Air Asia 8501) (Lande 2014). Other, less public prone LOC accidents occur in the business jet, special purpose and general aviation fleet segments. Training for LOC depends on specific flight operation characteristics, such as operating environment (weather conditions), aircraft characteristics (configuration, cruising speed and altitude, cockpit layout and ergonomics) and pilot induced oscillation (attention, distraction, experience and qualification).

In the low speed region, aircraft are sensitive to loss of control by aerodynamic stall, where the critical angle of attack should provide sufficient lift to remain airborne. In the high speed region at high altitude, margins between minimum and maximum airspeed become small. Attempts to maintain altitude may result in aerodynamic buffeting and subsequent high altitude stall due to limited engine climb power. This region is known as the 'coffin corner'. In commercial aviation, standard recovery training from stall is to apply power to minimize altitude loss, while the aircraft is sensitive to generate gyrating pitch.

Several authors criticize current stall recovery approaches: the simulator aerodynamics modelling is questionable, while recovery relies on piloting skills. A transfer from manufacturer product liability to operator training liability has taken place (Den Hertog 1999, Lande 2014, Veillette 2012). Such a 'dumping ground' design philosophy with an emphasis on operators responsibilities has created a need for sophisticated operational safety concepts such as Line Operations Safety Audit, Flight Operations Quality Assurance and Safety Management Systems. Simultaneously, such a transfer causes a loss of 'know why' on design decisions and assumptions (Den Hertog 1999).

Sources for LOC are multiple (Veillette 2012). Physical sources are a constrained manoeuvring space and a loss of situation awareness regarding the total energy balance of the aircraft, combined with true airspeed, banking angle, turning radius and contaminated wing surfaces. Mental sources are cockpit mismanagement, pilot induced oscillation, spatial disorientation and timely detection of a situation. LOC occurs frequently in Non Routine Flight Operations during post-maintenance, non-revenue flights or operating in the margins of the flight envelope. which are not covered by adequate training on problem scenarios. In flight control malfunction may occur generic due to freezing or chafing of controls, or by type specific control issues that are not tested and documented in regular certification procedures. Meteorological conditions which are not fully understood and predicted may create LOC events due to low level wind shear, wake turbulence, vortices rebound and mountainous waves due to updraft and downdraft. In the upper regions of the atmosphere, where small manoeuvring margins exist and LOC accidents are major hazard. Flying should be avoided in intertropical convergence zones which create super storm cells, thunderstorms and microbursts. In particular business jets, who fly higher and faster than commercial aircraft (M0.9 at FL 510 with clean wing configuration) are sensitive to LOC. Applying standard high upset recovery practices by giving power and maintaining pitch attitude, are sensitive to LOC accidents by high speed stall (Veillette 2012).

In general, LOC events have high dynamics. Detection, decision-making, reaction are in milliseconds, under high workload conditions, with a rapid development of the event, accompanied by abrupt automation disconnection, submitted to type specific flight handling properties and responses. Designing a failsafe solution, exclusive reliance on prevention is impossible. Stall and Loss of Control are inherent risks of flying and remain an inherent frontier to manage resilience in aviation. Consequently, recovery and resilience have to be built into the flight performance at the design phase.

3 INTUITIVE DESIGN

In the cockpit, the Primary Flight Display provides the physical interface between the aircraft flight mechanics and human performance. In the design of this display, the rational logical human cognitive and decision making model, based on formal logic and mathematical algorithms are the design standard. Several major accidents have revealed limitations in dealing with unanticipated and non-normal situations. External, contextual conditions are not taken into account, while internal reasoning processes are also controlled by intuitive, empathic and social dimensions.

An intuitive human performance model is advocated, based on the following assumptions (Lande 2014) :

- Pilots are relatively autonomous, context and condition dependent operators, dealing with both normal and unanticipated non-normal situations on a frequent and regular basis
- They participate in a traffic process control in a network configuration with distributed and delegated responsibilities
- Their decision making processes deal with safety critical aspects in a hierarchical order -aviate, navigate, communicate and manage- and basic control parameters –power, pitch and performance-
- Their decision making and control processes covers all phases of perception, recognition, interpretation and action perspectives
- Their decision making processes cover both rational, professional and formal logic decision algorithms and intuitive, empathic, emotional, communication and social dimensions.

Conventional man-machine interface designs are limited by risk mitigation strategies in which manufacturers and certification authorities apply the classic concept of 'workload' and transfer of manual flying tasks to high reliable automation as a remedy for 'human error'. There are sobering lessons on the effects of further automation: workload is not reduced but changed in nature or shifted, erroneous actions are not eliminated but may change in nature, and the usefulness of automation is questioned in terms of benefits versus new risks (Hollnagel, Cacciabue and Bagnara 1992). Such automation induces reduced need for pilots in flying skills training and proficiency, avoiding operations in the margins of the flight envelope (Lande 2014). However, experiences from the field demonstrate that such a conventional approach creates an illusion of a failsafe envelope protection and an inherent inability to stall, while discrepancies remain between the operating and training envelopes. Such conventional automation takes the pilots out of the control loop, hampering interpretations of cues and observables of primary flight parameters, intuitive inceptors and aircraft state transitions. In this conventional design approach, fundamental understanding of flight mechanics is also hampered by the absence of total energy management oversight and angle of attack indicators (Lambregts 1982). Taking the pilot out of the loop dissociates the pilot from proactive situation assessments in 'flying ahead of the aircraft'. Consequently, loss of situation awareness may occur in recognition of the vicinity of performance margins, display and mode confusion, loss of tactile and emotional feedback and composure in critical situations. Such loss should be compensated by Good Airmanship principles (De Crespigny 2012)

In addition to external oriented 'ecological' interface design, 'intuitive' design of the primary flight display is advocated facilitating pilots to deal with flight mechanical and human performance characteristics by a dedicated interface design (Lambregts 1982, Den Hertog 1999, Lande 2014). Such intuitive design should incorporate aerodynamic and flight dynamics basic knowledge, piloting skills and Primary Flight Display ergonomics.

4 INNOVATIONS FOR RESILIENT ENGINEERING

In a series of projects, based on a combined analysis of safety investigations, a historical survey of innovative approaches, scientific research on human performance and experimental setups, more fundamental issues were revealed in a better understanding of HMI architecture in dynamic control of aircraft:

- Introduction of redundancy on all primary flight control functions, in particular on pitch control, introducing technical redundancy in case of damage, malfunction or emergency
- Increasing resilience by decoupling of aerodynamic performance and centre of gravity range functions, leading to a configuration change from Tube And Wing into a class of Blended Wing Body aircraft
- Increase in responsiveness to preserve control over the aircraft in case of non-normal flight, degraded states and emergency handling as an answer to procedural flight restrictions.
- In order to achieve changes, a fundamental shift in focus is inevitable, creating resilience at an innovative level of research findings and patents on:
- Strategic decision making support by the introduction of a Total Energy Management based control system, dealing with the total energy rate and energy rate distribution of the aircraft (Lambregts 1982)

- Introduction of an angle of attack as a primary flight display in the context of a human factor centred approach, including its ergonomic cockpit layout and intuitive design features (Lande 2014)
- Introduction of a recovery shield as a redundancy in pitch control by enhanced physical control over aerodynamic forces in a 4 D operating environment, supported by computerized rapid deployable recovery shields, as an independent fall-back for the regular FMS (De Kroes 2011).

Flight safety by further development of the flight envelope protection is served by the introduction of a recovery shield (De Kroes 2011). These generic notions are applied to the recovery shield:

- redundancy. The implementation of a recovery function for pitch control is necessary because of the loss of aerodynamic forces on the aircraft by disruption of the air flow across the wing and empennage. In addition, malfunctioning of the regular control surfaces may occur due to external or internal damage, failure of control actuators or as collateral damage due to other malfunctions such as structural collapse. Such a recovery function focuses on technical redundancy. Additional redundancy is provided by an overlap between technical redundancy and enhanced emergency handling capacity of the pilot in the recovery control mode of the flight management system

- resilience. The decoupling of a tight relation between the aerodynamic center and center of gravity range of the whole aircraft can create a more flexible range for the aerodynamic center by adding two small eccentric forces, deployed by two small extractable control surfaces. A further optimization of the center of gravity range is possible beyond the conventional cg range, facilitating a more economic and flexible use of the aircraft. This device does not replace the elevators, but reduces their size, reducing weight and parasite trim drag. Such resilience focuses on performance efficiency and eventually may lead to reconfiguration of the aircraft geometry as foreseen in the EU Framework program of smart wing development or into new concepts such as the Beechcraft Starship and application of canard wings

- responsive. There is a growing concern in the pilot community with respect to the reduction of flying and emergency handling skills under automated flight conditions and continuing degree of automation. Such a transfer from pilot controlled recovery action to aircraft controlled recovery devices seems the only option for commercial aircraft in the absence of the powerful thrust vectoring which exists in military aviation. In such a strategy, a human centered design in maintaining overall control over the situation seems preferable over a fully automated solution. The focus is on redistribution of the decision authority between aircraft and pilot and requires careful design of the man-machine interfacing. Such a transfer is to be accompanied by a simulator training program. By making the aircraft-pilot interface more responsive to degraded flight conditions and emergency conditions, the aircraft becomes less dependent of fluctuations and unforeseen situations in normal conditions. Such a responsiveness may reduce planning continuation errors and procedural flight performance (De Crespigny 2012).

In order to introduce such innovations, several transition strategies have to be applied simultaneously:

- change from descriptive and explanatory variables towards change and design variables
- change in focus from events and factors to systems and vectors
- change from human error notions to Good Airmanship principles
- change from control terminology and notions to engineering design language and principles
- identification of game changers as critical agents to identify market niches, economic constraints, feasibility and lead time considerations.

Innovative design consists of new concepts in handling flight dynamics and control of the aircraft. A multi-layered Loss Of Control mitigation strategy is required to cope with both man, machine and their interface.

In such an innovative design, three conceptual restrictions in present aircraft design have to be eliminated:

- adding a second line of defence for the aerodynamic recovery in pitch control and aircraft handling by introducing the physical device of the ‘recovery shield’ (De Kroes 2011)
- loosening the tight coupling between aerodynamic centre and centre of gravity range to improve the lateral stability control range in non-normal situations
- make the transition from a classic formal logic and Tayloristic pilot control model towards a human centred design of ’intuitive’ interface design.

The feasibility of the project will be demonstrated with an integral and innovative design of a dedicated emergency and rescue aircraft: the Water Bomber.

5 AERAIL FIRE FIGHTING: THE WATER BOMBER

Over the past decades, aerial firefighting has evolved from conversion of military aircraft to special purpose applications in recue and emergency missions to designing dedicated aircraft configurations (DSE 2014). Such an evolutionary development has drawbacks in the efficiency and effectiveness of converted designs. Present water and fire retardant dropping strategies are risky and have a short lived effect in short passes. Serious accidents have occurred, despite the very skilled pilotage of former naval and aerobatic pilots. Aircraft such as the Bombardier CL-415 are capable of scooping 6 m3 of water at a speed of 130 km/hr in 12 seconds in a 400 m run, but date from 1993 and are to be replaced by a next generation of special build utility aircraft. Top level requirements aim at multifunctional aircraft for rescue and emergency, firefighting, relief and evacuation purposes. The design aims at an aircraft of an amphibious nature with STOL characteristics, high scooping capacity, removable hold configuration for equipment and excellent handling qualities for low altitude, low speed and all weather conditions. The aircraft operates in complex terrain situations in mountainous areas, forests, near oil rigs, highways and other high risk, aggravated operating conditions. Sudden scooping and release of large loads requires robust, reliable dynamic behaviour and fast, adaptive control characteristics. To fulfil such a wide and flexible range of functionalities, the aircraft will be a modular design. Certain modules are deemed necessary for the aircraft handling and operations, while others are optional for specific missions. With a modular design, clients have more freedom to design, repair and update the aircraft for specific functions and missions (DSE 2014).

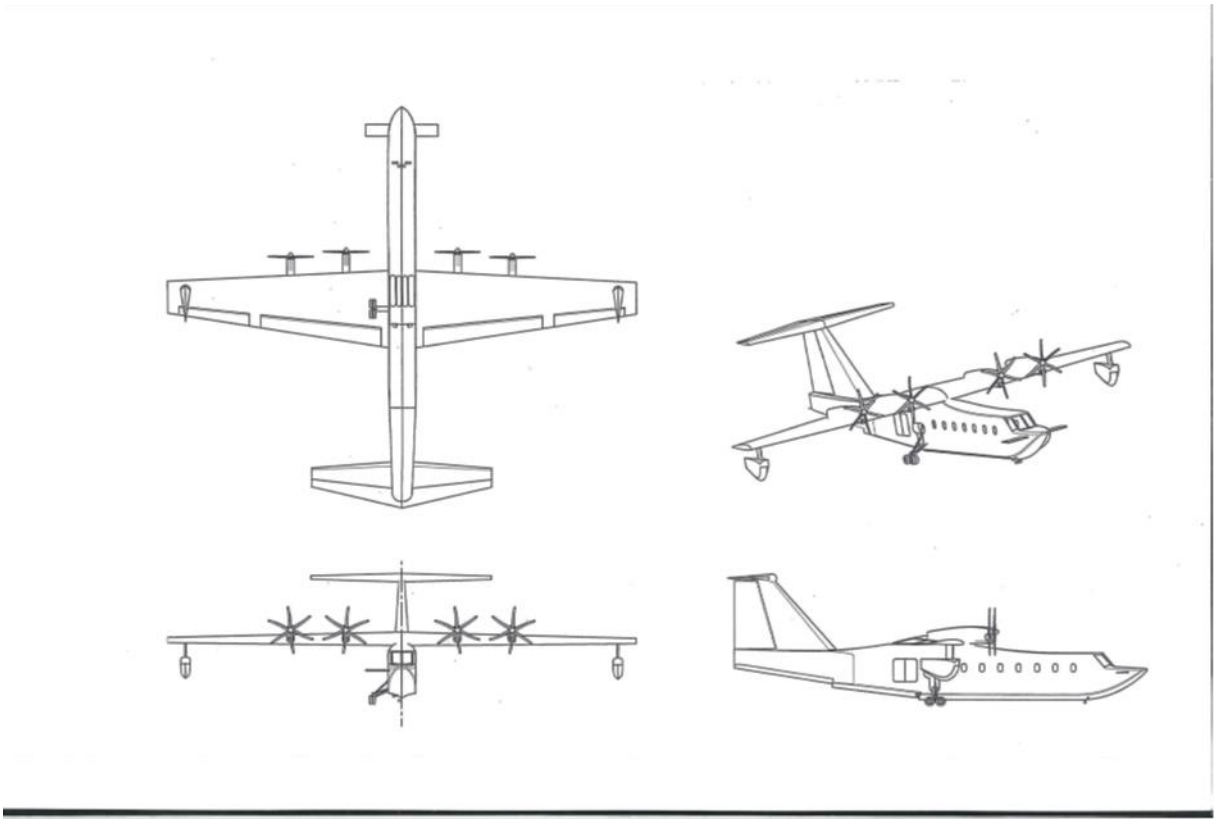


Figure 1: Water Bomber preliminary design

The price of the aircraft will vary, dependent from basic to enhanced versions. Such an adaptive and flexible design creates the necessary resilience for operations and sets the aircraft apart from previous generations. An integrated set of innovations contain the basics of the amphibious platform function with hydrofoils, control canards, electrical actuation of control surfaces, inflatable or retractable wing tip floats and intuitive cockpit design. Mission specific innovations cover functionalities regarding water cannons, multiple types of retardant and multiple, swappable retardant tanks and CADAS, the Computer Augmented Detection and Aiming System. The introduction of location based 3D printing of spare parts and components serves increased maintainability and flexibility in field operations.

6 CONCLUSIONS

The contribution demonstrates the practical application of resilience engineering to the design community in aviation. Feedback from reality -such as safety investigations and accident scenario thinking- is practically applicable in an empirical approach of such a complex phenomenon as stall and LOC prevention. In addition to the design requirements for a sustainable and resilient approach to stall and LOC, system change drivers and change agents are identified as constraints and operating conditions imposed by higher system level dynamics. Coping strategies with safety performance of the overall system beyond the level of robustness, redundancy and reliability are identified, identifying niche markets, fleet segments and macro-economic conditions for a sustainable development of innovative solutions. In addition, several conceptual changes have to be made regarding the human behaviour modelling, the role of automation and a discrimination between a focus on event occurrence and system change. The contribution also indicates the potential for safety investigations to serve as input for resilience engineering practices, considering stall and LOC scenarios as the ultimate load concept for system failure identification and type certification. Since stall is an inherent property, it forms an inherent frontier for managing resilience. A retrospective approach remains indispensable.

Finally, involvement of aerospace students and the use of patents in the project highlights the potential for engineering design initiatives to get acquainted with resilience engineering principles and concepts as a perspective to create innovative and integral solutions.

REFERENCES

De Crespigny R. (2012) QF32 *The captain's extraordinary account of how one of the world's worst air disasters was averted. Macmillan*, Pan Macmillan Australia.

Den Hertog R. Safety starts at the Manufacturer. Presented to the Netherlands Association of Aeronautical Engineers (NVvL) on May 27, 1999

DSE Water Bombers. (2014) *Towards a Next Generation of Water Bombers. Final Report Design Synthesis Exercises.* Delft University of Technology. Aerospace Engineering, Jan 2014

De Kroes J.L. (2011) Patent 2008049. *Subsonic plane or flight simulator thereof, adjustable fuselage control surface, computer program product and method.* Jan L. de Kroes

Hollnagel E., Cacciabue P. and Bagnara S. (1994) *The limits of Automation in Air Traffic Control and Aviation. Report from a Workshop held at Certosa di Pontignano,* Italy, November 25-27, 1992.

Lambregts A. (1982) Patent US 4536843. *A Total Energy based flight control system.* Antonius A. Lambregts

Lande K. (2014) *Aircraft Controllability and Primary Flight Displays – A Human Factors Centred Approach.* European 46th and 25th SFTE Symposium, 15-18 June 2014, Lulea, Sweden

Stoop J.A.(2013) *Towards a failsafe flight envelope protection: the recovery shield. Advances in Risk and Reliability Technology Symposium* 21st – 23rd May 2013 Loughborough, Leicestershire, UK

Veillette P. (2012*) Investigating and preventing the Loss of Control Accident*. ISASI Forum July-September (Part 1) and October-November (Part 2) 2012.

ERGONOMICS AND CREATIVITY IN A HIGH PRESSURE AND UNPREDICABLE WORLD (workshop)

Teresa Cotrim 1 and Sara Albolino 2
1Faculdade de Motricidade Humana, Universidade de Lisboa, Portugal
1 tcotrim@fmh.ulisboa.pt
2 Center for Patient Safety – Tuscany Region, Italy
2 sara.albolino@gmail.com

Abstract

Understanding real work and systems operations plays a fundamental role in resilience engineering, which renders ergonomics and human factors practices particularly relevant for advances in this domain.

The main objectives of the workshop are: starting a debate among professionals of different fields about the more effective way to develop creativity in practice, through the use of ergonomics in order to reduce costs and improve quality and safety in different domains of working life and leisure; sharing of creative and innovative solutions developed in specific fields through the use of ergonomic methods; identification of specific issues to be addressed by the research activities, in the ergonomic field, in order to develop the topic of creativity in practice.

The concept of creativity in the actual international context, where the socio-economic situation is unstable and unpredictable, is a strategic concept to develop new resources to face critical scenarios nowadays and in the future.

The concept of creativity, related to ergonomics, needs to be intended in a broad way and includes, besides the design also sectors as the craftsmanship which represents a key process in the new tendencies of globalization, it considers actual contexts and constraints and potentialities that define environments and activities, human beings and technology, identities and cultures. Creativity in practice is an inherently evolving topic in which prospected solutions are necessarily adaptive to continuously changing contexts.

Any unforeseen use of a product is a source of uncertainty to designers. It can be viewed as a source of hazards to the user, system or environment or as a potential source of innovation. In this process, creativity can be identified as a value and ergonomics gives a conceptual framework.

Ergonomics is the science and discipline that supports, with its approach, methodology and techniques, the challenge to build solutions that can be at the same time innovative and competitive from the economic point of view in the different sectors such as healthcare, design, occupational health, communication.

Questioning if ergonomists are able to be creative and to produce work that is both novel and appropriate is one of the challenges of the workshop.

The workshop anticipates the topic of IEA2018 aiming at opening the debate among professionals around this theme and introduce some of the main issues to be developed over next years.

LEVERAGING RISK REGISTER INFORMATION FOR DEVELOPING RESILIENCE THROUGH RISK INTELLIGENCE (poster)

M.C. Leva [1] and N. Balfe [2]
[1,2] Centre for Innovative Human Systems, Trinity College Dublin, Dublin 2
[1] levac@tcd.ie 00353-1 896 2916
[2] balfen@tcd.ie 00353-1-896-3576

Poster abstract

Resilience can be defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel, 2011). Central to this definition is the core ability of an organization to understand, monitor and develop a risk intelligence capacity.

A risk database, or risk register, is a central tool for organisations to use to monitor and reduce risks, both those identified during initial safety assessments and those emerging during operations. The risk register should contain all analysed risks and should prioritise the areas that require managerial attention. When populated with information on each risk, including risk ranking, the risk register can be analysed to present the risk profile for different aspects of the organisation. When reviewed and updated over time, it can also be analysed to present trends within the risk profile and focus management attention on the highest risk activities or facilities. This research presents a concept of extending traditional risk registers through analysis of the information contained within them across an entire company (data-mining) to develop risk intelligence in order to support resilience.

1 SUMMARY OF THE PROPOSAL

The poster will present a concept of building risk intelligence to support resilience in safety critical industries using data from a risk register. The case study presented is from an electricity generation company, who have identified the need to better manage their safety and resilience information and have developed a comprehensive risk register containing information on technical, human, financial, environmental, and regulatory risks across the entire generation business. Electricity generation is an inherently high energy, multiple hazard industry that can potentially be harmful to life, health, assets, and the environment. The presence of this stored energy or hazardous substances, which when released can cause damage, can take many forms including, chemical, mechanical, thermal, electrical, etc. Process safety is concerned with preventing harm to people, the environment and the plant from this uncontrolled release of energy / hazardous substances through a combination of good engineering design / practices, asset and integrity management, and through good operation and maintenance practises (Hopkins, 2009). The company involved in this research operates a number of electricity generation stations and has an on-going programme composed of a multiple of projects to improve process safety.

In order to maintain safe operations, organisations must continuously review and monitor their risks. This means that the results of safety studies must be translated into a format that can be analysed, reviewed and acted upon, and new data about the level of risk continuously collected to keep the safety information up to date. A risk database, or risk register, is a central tool for organisations to use to monitor and reduce risks, both those identified during initial safety assessments and those emerging during operations (Whipple and Pitblado, 2010). The risk register should contain all analysed risks and should prioritise the areas that require managerial attention and typically contains information describing each risk, an assessment of the likelihood and consequences, a ranking according to a risk matrix, the risk owner, and information on the mitigations to be put in place (Filippin and Dreher, 2004). When populated with information on each risk, including risk ranking, the risk register can analysed to present the risk profile for different aspects of the organisation (Filippin and Dreher, 2004). When reviewed and updated over time, it can also be analysed to present trends within the risk profile and focus management attention on the highest risk activities or facilities (Whipple and Pitblado, 2010). In order to successfully develop a risk registry that provides an accurate level of risk within a process, there is a requirement for real time data on risk to be input into a risk registry.

The risk register developed as part of this research allows individual stations to document and monitor their

risks and to report upwards their priority risks (Balfe, Leva, McAleer & Rocke, 2014). However, the benefits are limited when confined to individual stations; this poster explores the potential to use the information captured for developing risk intelligence through data mining of the risk registers and sharing of risk information across sites. This approach can help develop overall resilience by facilitating learning across sites, improving the ability to anticipate risks, and monitoring risk profiles across the business. The poster will present the proposed approach, based on the existing risk registers.

The risk intelligence developed through mining the data collected in company-wide risk registers can provide advanced support to the organisation to manage resilience. The sharing of information between sites means that different stations can proactively anticipate threats that have not yet manifested symptoms in their station, learning from the experience of others. The information on mitigation actions held within the risk registers help the organisation adapt, using the database to adopt successful mitigations to evolving risks.

REFERENCES

Balfe, N., Leva, M.C., McAleer, B. & Rocke, M. (2014). Safety Risk Registers: Challenges and Guidance. Chemical Engineering Transactions, 36, pp. 571-576.

Filippin K., Dreher L., 2004. Major hazard risk assessment for existing and new facilities. Process Safety Progress, 23, 4, 237 – 243.

Hollnagel, E. (2011). Prologue: The scope of Resilience Engineering and Epilogue: RAG – The Resilience Analysis Grid. In: Hollnagel E., Pariès, J., Woods, D.D., and Wreathall, J. (Eds.), Resilience Engineering in Practice: A Guidebook. Ashgate, Aldershot, UK

Hopkins A., 2009. Thinking about process safety indicators. Safety Science, 47, 4, 460-465.

Whipple T., Pitblado R., 2010. Applied risk-based process safety: A consolidated risk register and focus on risk communication. Process Safety Progress, 29, 1, 39-46.

SolvingTensions (poster)

Airol VTT
Nieminen VTTT

A CASE STUDY: SOLVING TENSIONS AS A WAY OF ENHANCING ADAPTIVE CAPACITY, RESILIENSE AND BUSINESS CONTINUITY

Airola Merja & Nieminen Mika
VTT Technical Research Centre of Finland Ltd

Introduction

The operating environment of firms is in constant change due to the effects of globalization and new technologies. In order to survive under these circumstances organisations need a paradigm change. New practices and abilities must be developed both on organisational and individual level. Organisations should be viewed as complex adaptive systems. They consist of diverse agents that learn and interact with each other in nonlinear ways. (McDaniel 2007; Stacey 2010, 2012). Companies as complex adaptive systems are practically impossible to manage in the traditional sense of the word. Instead of detailed planning and controlling, an organisation should aim to develop its resilience and self-organization capacity (Berkes 2007; Lichtenstein et al. 2006; Nemeth & Hollnager 2014). In order to understand the functioning of organisations as complex adaptive systems research should be directed increasingly towards their emerging action patterns and agents' interactions (Eoyang & Holladay 2013).

Data and methodology

In this paper, we investigate the challenges of enhancing resilience and adaptive capacity in the context of a Finnish high tech SME. The company operates in the field of energy technology. The study focuses on understanding tensions affecting resilience and adaptive capacity and their effects on the continuity of business. The study was conducted by interviewing CEO and middle managers and key persons in the firm (altogether 17 persons). The case company has gone through rapid growth and decline in the global market.

Adaptive capacity is a measure of the culture and dynamics of an organisation that allows it to make decisions in a timely and appropriate manner.

We categorized the relevant action patterns of the firm as follows: leadership and decision making structures, perception of the organisation strategy, the acquisition, dissemination and retention of information and knowledge, and the degree of creativity and flexibility which the organisation promotes or tolerates. Patterns, in turn, involve tensions that initiate and enhance change and development in the system (cf. Reiman, T. et al. 2014) (Figure 1.)

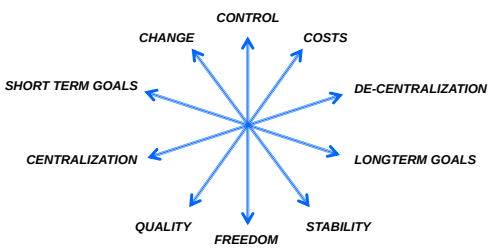


Figure 1. *Tensions.*

Results

Our results indicate, how tensions and dysfunctions between different organisational levels are maintained and reinforced. The notions of the unintended and unconscious outcomes of managerial actions are examined (see Table 1.)

Table 1*. Results.*

	Action patterns and related tensions
Leadership and decision making structures	▪ Top down management and leadership in the economic turbulence. Contradictory ideas about organisation and how it functions. On the one hand it seems that all the power lies with the CEO – on the other hand experts are able to make independent decisions regarding their expertise area. ▪ Centralized, not transparent decision making structures even regarding to small purchases. ▪ Tension are maintained and reinforced by division of the organisation as insiders like-minded with CEO and outsiders.
Perception of the organisation strategy	• Widely shared and accepted company story created and reinforced by top management team. • The strategy seemed to be lost in the time of the survival mode – the great story held the organisation together. • Tensions are maintained by the top management perception that middle management is not aware of the critical economic situation and therefore not committed to the company strategy. According to middle managers there is no space for even constructive criticism.
Acquisition, dissemination and retention of information and knowledge	• Top management ability to react quickly to market changes and inline to the market changes. Middle managers ability to adapt quickly to changing customer needs. • Tensions are maintained by the lack of efficient coordination and contradictory of customer needs. • Top management refers that there is a lot of information and discussions - middle managers agrees about the information, disagrees that there is discussions. • No time or resources for renewal of the organization.
Degree of creativity and flexibility which the organisation promotes or tolerates	• In the middle management perspective there is not enough resources for R&D that enables innovation and maintenance of competitive advantage. Top management slightly disagrees and has emphasis on the economic conditions. • On the other hand organisation promotes flexibility and the actors are able to outdo themselves in the customer work and customization. On the other hand there is lack of connections and communication to boots the activities towards the shared goal.

Conclusions

Organizations are evolving through tensions. Although the leaders have made in this case several successful actions to ensure the resilience of the organization under market pressures, there are also unintended consequences for these actions, which, in turn, undermine the overall resilience of the organization. Tensions should be made visible through communication and interaction between organization levels and stakeholders.

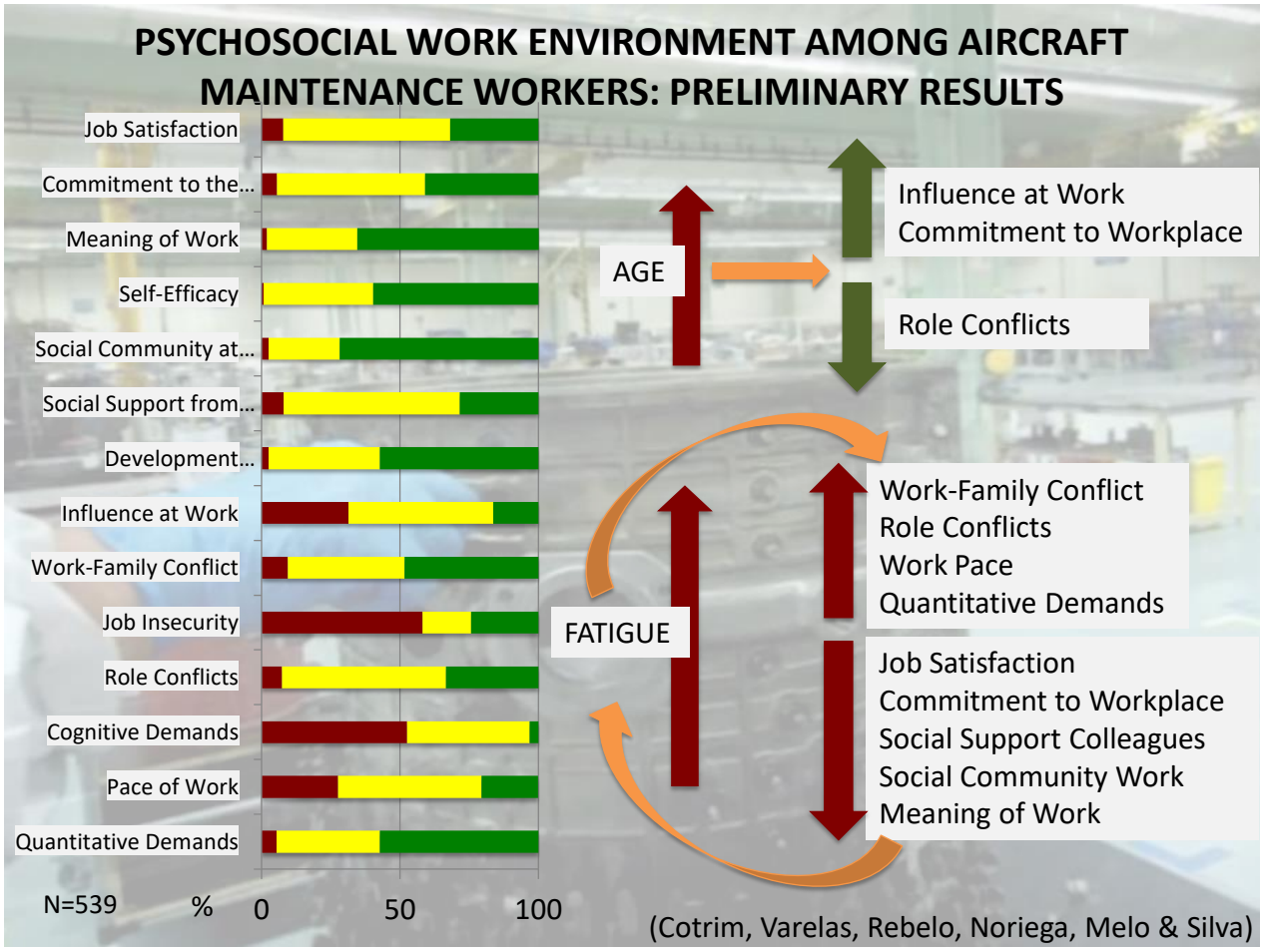
Contacts

Merja Airola
Tel. +358 50 525 1655
merja.airola@vtt.fi

Mika Nieminen
Tel. +358 40 159 0283
mika.nieminen@vtt.fi

PSYCHOSOCIAL WORK ENVIRONMENT AMONG AIRCRAFT MAINTENANCE WORKERS (poster)

Cotrim etal



CRITICAL STEPS (Poster)

Muschara

CRITICAL STEPS

Managing Human Operations That Must Go Right Every Time

Tony Muschara, CPT

Muschara Error Management Consulting, LLC, 4724 Outlook Way NE, Marietta, Georgia 30066-1790 United States | tmuschara@muschara.com

Muschara Error Management Consulting, LLC

1. What is a Critical Step?[1, 2]

Critical steps make safety boundaries of assets explicit in an operation, where they can experience harm due to work. Work requires human touchpoints to initiate transfers of energy, movements of mass, or transmissions of information. As points of no return, critical steps are tight coupling situations intolerant of error—single-error vulnerabilities. Words used to define a critical step (definition at right) are descried below:

- Asset – things valued by an organization important to the organization's mission and purposes
- Inherent hazards – sources of energy, mass, and information designed into a process with the intent to add value during production or services
- Human Action – one human interaction with an asset or hazards that triggers an unwanted outcome (harm); loss of control in close proximity to an asset or hazard (touchpoint)
- Will – no uncertainty that harm will occur; no doubt
- Immediate – harm ensues after loss of control; harm realized within moments of action, whether recognized or not by the performer; consequences occur faster than people can humanly respond to avoid the the onset of harm
- Irreversible – no undo; cannot return to original, previous, unharmed condition by simply reversing the initiating action; point of no return
- Intolerable Harm – worst case outcomes related to key assets involved with an operation; serious unwanted effects; not always self-revealing; reserved for actions that trigger serious harm

A human action that will trigger immediate, irreversible, intolerable harm to an asset, if that action or a preceding action is performed improperly.

2. Man Says Hold the Cheese...*

A man in his early 20s orders two hamburgers without cheese at a drive through window of a local fast food restaurant. This young man has a life-threatening allergy to cheese. However, after receiving his order, he does not check that the hamburgers have no cheese. He assumes there is no cheese on his order since he had mentioned it five separate times in ordering as he stated afterwards to a news reporter. Later, after dimming the lights to watch a movie, he bites into one of the hamburgers and swallows the food. He does not taste the cheese. Immediately, he suffers a severe allergic reaction to the cheese. Fortunately, some family members are with him, and they rush him to a nearby hospital in time to save his life. Taking that first bite and swallowing the food was the point of no return, and it almost cost him his life.

* Adapted from Anderson, J. (August 10, 2007). "Man says hold the cheese, claims McDonald's didn't, sues for $10 million," Charleston Daily Mail.

3. Examples of Critical Steps

- Breaching a pressure boundary (pipes and tanks)
- Entering a confined space (atmosphere)
- Taking a bite of a hamburger (for someone allergic to cheese)
- Opening or closing a circuit breaker (electricity)
- Making an incision (surgery)
- Clicking "Send," "Open," "Start," "Go," or "Enter"
- Crane operator taking tension on a heavy lift
- Opening the bottom valve on tank containing cancer-treatment drug substance on a fill line
- Leaping out of the door of an airborne aircraft (skydiving)
- Entering the line of fire (direct exposure to a hazard you have little or no control over)
- Pulling the trigger on a firearm

4. TouchPoints (exposures: human couplings with assets)

A human interaction with an object (asset) that changes the state of that object through work

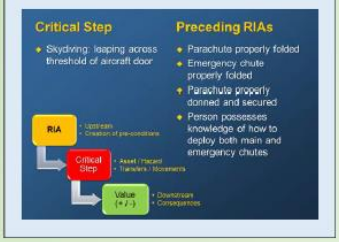
Work involving:
- Transfers of Energy, or
- Movements of Mass, or
- Transmissions of Information

5. What is a Risk-Important Action (RIA)?

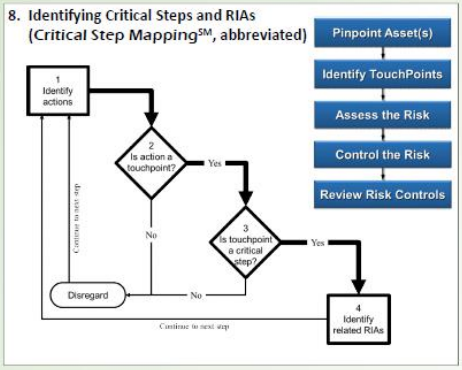
6. Examples of Risk-Important Actions (RIA)

- Donning personal protective equipment
- Pressurizing a tank
- Hovering cursor over "Send," "Start," or "Enter"
- Checking a hamburger for the presence of cheese (for someone allergic to cheese)
- Climbing a ladder
- Securing the drain plug during an oil change of an automobile
- Stopping at a Stop Sign
- Verifying initial conditions specified in a chemical process procedure
- Taking the safety off on a handgun

7. Linkages Between Critical Steps and Risk-Important Actions (RIA)



8. Identifying Critical Steps and RIAs (Critical Step Mapping℠, abbreviated)



9. Risk-Based Thinking[3]

Risk-based thinking provides a logical approach to deciding what to do for safety, especially when one must adjust to local conditions inconsistent with procedures. Risk-based thinking is usually preceded with a sense of uneasiness about a specific operation. People with a chronic uneasinesse possess a deep-rooted respect for the technology, assets, and inherent hazards as well as a mindfulness of their own fallibility. Such feelings provoke a search for facts, which risk-based thinking facilitates through the following mental practices:

- **Anticipate** – know what to expect (accomplishments/assets)
- **Monitor** – know what to pay attention to (critical steps)
- **Respond** – know what to do (positive control*)
- **Learn** – know:
  - ✓ what has happened (past)
  - ✓ what is happening (present)
  - ✓ what to change (future)

*** Positive Control** – actions to ensure that "what is intended to happen is what happens, and that is all that happens."

10.Enhancing Positive Control of Critical Steps[4]

RU-SAFE℠ – A dialogue that promotes risk-based thinking among co-workers about what to accomplish and what to avoid prior to starting work:

1. **Recognize** assets involved in operation
2. **Understand** hazards to those assets and lessons learned
3. **Summarize** critical steps and related risk-important actions
4. **Anticipate** errors traps and errors for each critical step
5. **Foresee** consequences of errors at each critical step
6. **Evaluate** Hu Tools, contingencies, and STOP-work criteria

Self-Checking (STAR)	Peer-Checking
1. **Stop** – prior to transfers of energy, movements of mass, / transmissions of information	1. **Performer** and **Peer** agree on action and expected outcome.
2. **Think** - understand what will happen, especially to assets, when performing the action	2. **Peer** prepares to observe and to correct.
3. **Act** – perform correct action on correct component	3. **Performer** and **Peer** self-check (separately).
4. **Review** - verify anticipated result obtained; otherwise, apply contingency or STOP criteria	4. **Performer** performs correct act on correct component.

11.What are You Going to Do About Critical Steps?

Safety is not what you have, it is what you do, especially at critical steps. There is no margin for error at a critical step—performance must be perfect. Critical steps always involve substantial transfers of energy, movements of mass, or transmissions of information, which could trigger serious harm if control of such operations is lost. Assets are protected from the harm triggered by human failures by 1) pinpointing assets needing protection during an operation, 2) identifying touchpoints, 3) assessing the consequences of a loss of control at each touchpoint (Is touchpoint a critical step?), and, then, 4) introducing means to exercise positive control at critical steps and their related RIAs that precede them. Workers improve their chances of controlling critical steps in an operation by participating in a dialogue before beginning work to address what is to be accomplished and what to avoid. Systematically identifying and controlling critical steps is an important safety function to incorporate into daily work processes. Such previews of high-risk work improves a work team's chances for success not only during expected circumstances but also during varying or unexpected situations by sensitizing them to what assets need protection and their hazards.

[1] Adapted from Center for Chemical Process Safety (1994). *Guidelines for Preventing Human Error in Process Safety*. New York: American Institute of Chemical Engineers. pp.209-211.
[2] The term "critical step" was adopted from Fischer, S., Konkel, H., Houghton, K., Wilson, M. (1998). *Identification of Process Controls for Nuclear Explosive Operations* (Report LA-UR 98-2246). Los Alamos: Los Alamos National Laboratory, U.S. Department of Energy. Retrieved from http://www.osti.gov/scitech/servlets/purl/296659/.

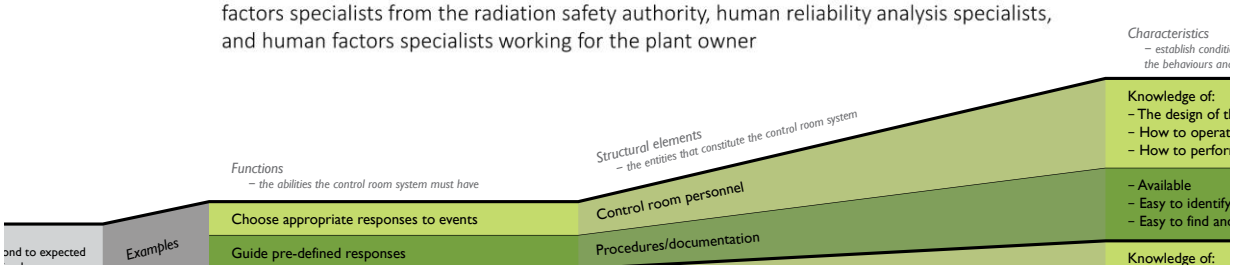
[3] Adapted from Hollnagel E. (2009). The Four Cornerstones of Resilience Engineering from Nemeth, C., Hollnagel, E., and Dekker, S. *Resilience Engineering Perspectives, Volume 2, Preparation and Restoration*. Farnham: Ashgate. pp.117-132.
[4] The human performance tools (non-technical skills) *Self-Checking* and *Peer-Checking* described on this panel were retrieved and adapted from the following U.S. Department of Energy (DOE) Website: http://energy.gov/sites/prod/files/2013/06/f1/doe-hdbk-1028-2009_volume2.pdf

THE CORNERSTONES OF RESILIENCE (poster)

Simonsen & Osvalder

Connection between the cornerstones of resilience and the design of control room systems

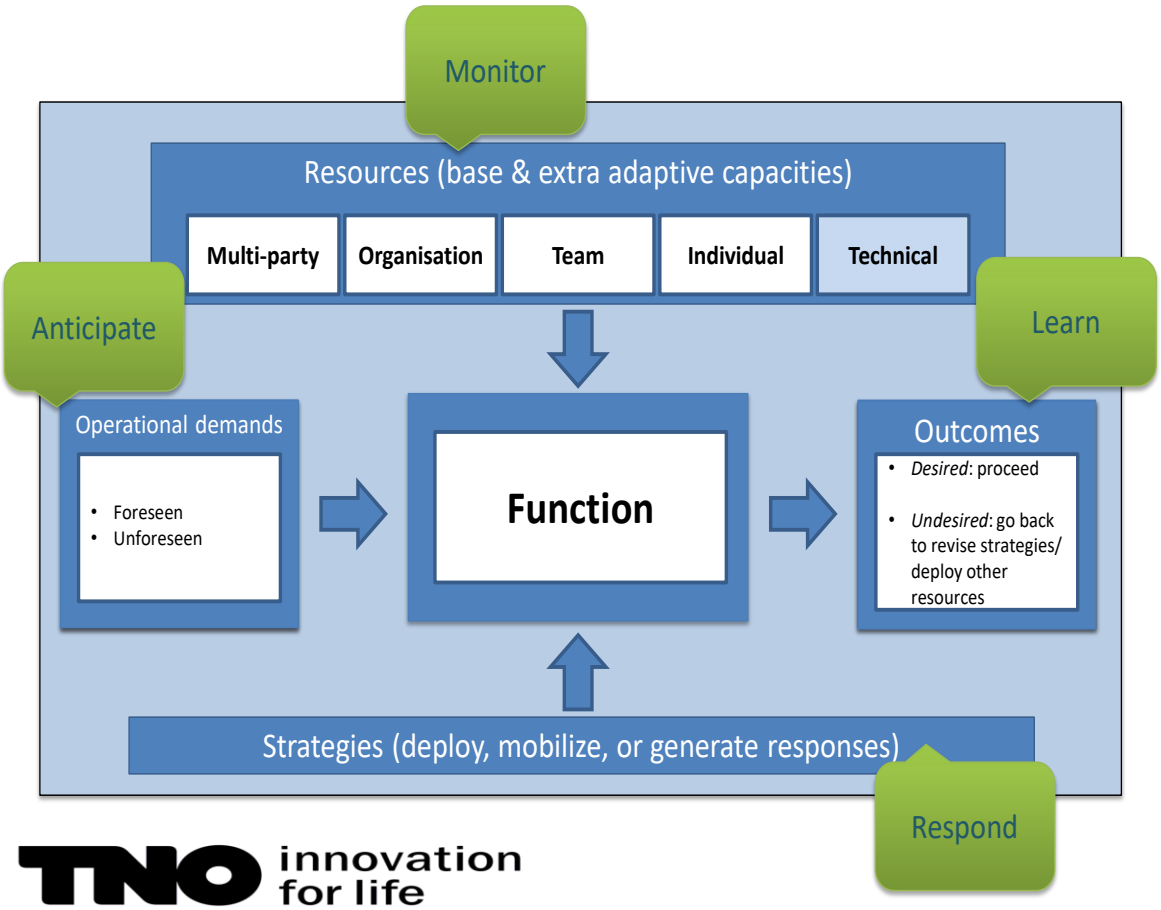
- In an unpredictable world, how can we design nuclear power plant control room systems to be adaptable and proactive?
- Aim of study: To explore how concrete aspects of the nuclear power plant control room system can be connected to the four basic abilities of resilient performance
- Interview study – *What contributes to safe operation*?
  - 14 interviewees: reactor operators, shift supervisors, instructors, inspectors and human factors specialists from the radiation safety authority, human reliability analysis specialists, and human factors specialists working for the plant owner



MULTILEVEL ASSESSMENT FRAMEWORK (poster)

Dolf vd Beek TNO

Multi-level Assessment Framework



TNO innovation for life

RESILIENCE ENGINEERING ASSOCIATION (REA)

The REA aims to develop a community of practitioners and users of Resilience Engineering
To create ways to share experience and learning, such as:

- summer schools and industry partnerships,
- conferences and workshops,
- books and papers.

To create a sense of identity:

- a collegial community of practitioners and users,
- a confederation of industrial partnerships,
- opportunities to speak with a common voice in professional and industrial settings.

To promote a shared understanding of what resilience engineering means:

- Linkedin group: http:/www.linkedin.com/groups/Resilience-Engineering-Association-REA-4610096/about
- debate and discussion, examples of applications in diverse ways and fields, point and counterpoint.

RESILIENCE ENGINEERING ASSOCIATION WEBSITE

http://www.resilience-engineering-association.org/

SYMPOSIUM WEBSITE

http://www.rea-symposium.org

CONTACT

info@resilience-engineering-association.org