Planning Measuring Resilience Potential and Early Warnings (SCALES)

I.A. Herrera[1], A. Vennesland[1], A. Pasquini[2] and S. Silvagni[2]
[1] SINTEF Information and Communications Technology, Strindveien 4, NO-7465, Norway
ivonne.a.herrera@sintef.no
[2] Deep Blue SrL, Via Lucrezio Caro 7/A, RM-00193, Italy
alberto.pasquini@dblue.it

Abstract. The central goal of SCALES is to link Resilience Engineering and Enterprise Architecture principles into a framework (the "SCALES Framework") that enables a context driven analysis of resilience. Enterprise architecture will offer the opportunity to model system of systems and to consider the system from different viewpoints (functional, communication, information and process view). For each viewpoint SCALES will identify appropriate resilience related indicators. These will be measured and monitored during system in operation, providing information about system ability to adapt to perturbations and maintain its functionality. This paper explains how the SCALES project will be organised to guarantee the achievement of these objectives and to ensure that its results are properly validated. Then, the relation to fundamental trade-offs is included. Finally, it invites to a critical discussion of the approach proposed and possible improvements.

1 INTRODUCTION

Traditionally, most safety indicators and metrics are related to deviations, failures or "after the fact" information. Since the seventies of the last century, the progressive improvement of safety methods relying on these indicators has certainly contributed to the excellent safety score of aviation. However, systems today are exposed to new changes that challenged the established approach to measure performance. These changes are the fast pace of technological change, the change in management structures, the changing nature of accidents, new types of hazards, decreasing tolerance for single accidents, increasing complexity, integration and coupling of systems, additional complex relationships between people and automation, changing regulatory and public views of safety (Amalberti, 2001; Dekker, 2005; Leveson, 2004; Woods, 2003; Rasmussen and Svenung, 2000). Moreover, the introduction of the ambitious improvements foreseen in the new Single European Sky will carry new challenges that the Single European Sky ATM (Air Traffic Management) Research (SESAR) is trying to address. These improvements are significant in terms of traffic

management capacity, safety and flexibility. Using advance technologies, the ATM system will have to be able to tolerate and adapt ensuring that performances are maintained in spite of inevitable perturbations. Since the system will be dynamically adapted to ensure user-preferred trajectories and demand-capacity balancing, the solely focus on accidents and incidents is inadequate for ensuring and monitoring these performances. New approaches for more proactive performance monitoring have been proposed in different industries: nuclear (Wreathall, 2006; Reiman and Pietikäinen, 2010); petroleum (Step-Change in Safety, 2001; Øien et al, 2010, Vinnem 2010) and aviation (Eurocontrol, 2009, Herrera, 2012). None of these approaches consider the combined challenges posed by SESAR.

Monitoring the performance of the system from a resilience perspective is required since it leads to interventions aiming to manage and adjust the adaptive capacity of the systems in face of inevitable disturbances. This requires an adequate representation of the system under analysis that in the specific of ATM can be so complex that it can be considered as a system of systems. Enterprise Architecture principles facilitate an effective modelling of such complex systems, roles, functions and procedures within and across organizations. Therefore, the central goal of SCALES is to link Resilience Engineering and Enterprise Architecture principles into a framework (the "SCALES Framework"). This framework shall enable a context driven analysis to measure the potential for resilience with respect to small and large perturbations. Our motivation is to take resilience engineering out of the pure academic setting and translate it into practical solutions in the real world. SCALES addresses the research question: *What added value can the combination of Enterprise Architecture and Resilience Engineering contribute to measure the resilience potential of the ATM system?*

SCALES will investigate the combination of Enterprise Architecture and Resilience Engineering that has not yet been explored in safety critical domains. The concrete outcomes will be a web tool and guidelines demonstrating how resilience related indicators can be identified and measured using different viewpoints of a system. Each viewpoint enables the analysis of the system from different angles (functional view, information view and process view). The Web tool will help resilience analysis offering an automated support that is still missing in the resilience domain.

2 METHOD

2.1 Combining Enterprise Architecture and Resilience Engineering

Enterprise Architecture (EA) is an architectural technique that is typically applied on complex environments, such as advanced systems or system-of-systems. It prescribes a holistic approach where the technology is not isolated from human and organizations; these aspects are treated equally important. Furthermore, separation of concerns and

abstraction are techniques that are applied in EA. Decomposing the total system into separate viewpoints, provides a global overview and detail when necessary that enables an immediate focus on relevant areas while reducing impact from irrelevant aspects.

An ATM system is typically composed of a number of complementary and interacting systems, such as regulators, airlines, aircraft operations, air traffic control systems and air traffic management and has the characteristics of a system-of-systems environment. Moreover, human and organizational involvement with such systems is critical. In a well-functioning ATM system workflow-based procedures and protocols as well as clearly defined responsibilities to be performed within and across systems are essential for safe operation. Hence, principles from EA should lend themself well to support a resilience approach because it supports the description of the system as the system works and its contextualization.

We will use the ARKTRANS (Wes, 2004) methodology to analyse and to identify resilience related indicators of the ATM system in a specific context. ARKTRANS is an EA variant that includes the following architectural aspects: *Roles*, *Functional Viewpoint*, *Process Viewpoint* and *Information Viewpoint*. Roles specify a delimited set of responsibilities and can be used to identify the relevant responsibilities of both systems and human actors. The Functional Viewpoint defines the functions that the roles must perform as a part of their area of responsibility. The Process Viewpoint defines procedures and protocols as well as information interfaces between roles and their functions. The Information View further details the information that is exchanged in the interfaces.

Resilience Engineering analysis will adapt resilience properties (Woods, 2006) and abilities (Hollnagel, 2009). The properties are buffering capacity, flexibility and cross scale interaction. These properties will extend the method Resilience Analysis Grid addressing the abilities that are analysed to monitor, anticipate, respond and learn (Hollnagel, 2011). The properties and abilities will be associated with a set of questions that need an answer to identify candidates for indicators. Buffering capacity questions relate to the size or kind of disturbances that the system can adapt maintaining operation. Flexibility questions address the possibilities of the system to restructure in response to external or internal changes and pressures. Cross-scale interactions questions relates to the influence of the context to local adaptations, and how local adaptation has an impact on more global, strategic goals. Monitoring questions address system performance and its possibility to identify what might become critical. Anticipation questions address threats and opportunities, not only single events but also how the system works and potential for cascade. Respond questions look into the ability of the system to cope with specific events (limited to the case studies). Learning

questions address if the system has learned from experience as reflected in practices and procedures.

This initial version of the framework will identify relevant and critical systems and human actors, required functions, procedures and protocols, as well as information exchange. This will be mapped to appropriate viewpoints of the initial framework. Associated with these viewpoints is a set of resilience properties, abilities and corresponding questions adapted from state of the art literature within RE. Combining EA and RE this way will enable an ATM system to be analysed in terms of *its resilience potential* as shown in figure 1.

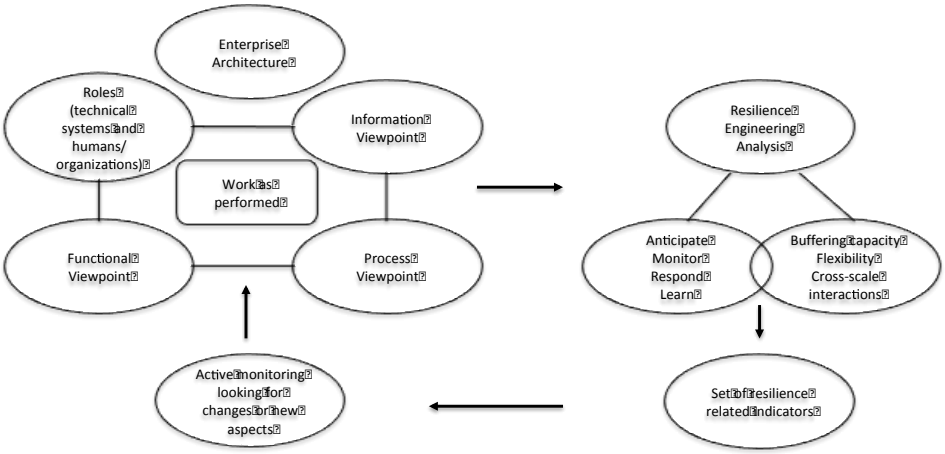

Fig. 1. Combining Enterprise Architecture and Resilience Engineering. It shows EA modelling and viewpoints. Each viewpoint will be subjected to a RE analysis considering resilience abilities, properties and corresponding questions to determine a set of resilience related indicators. These indicators must be actively reviewed looking if new critical aspects for operation need to be considered as situation changes.

So for example, in the Functional Viewpoint SCALES will define which functions a pilot (role) must perform in order to ensure good ability to respond to a potential event. In the Process Viewpoint the pilot role´s interaction with its environment is defined with respect to the sequence of functions performed by each role (e.g. pilot, air traffic control system, air traffic controllers, technicians) and how these roles and functions interact with other roles and functions. It includes, at which step of the workflow should the pilot communicate with the air traffic control system (role) and which information should be communicated (and when). The information being communicated in the interface between the pilot and the air traffic control system is then further defined in the Information View. Each of these viewpoints of the framework will be accompanied by a set of set of questions related to resilience

abilities, properties with corresponding questions that contribute to identify indicators related to (un) successful operation. Two type of operations are mapped in SCALES everyday successful operation and case studies (incidents).

2.2 Case studies and SCALES

In order to get trustworthy results the SCALES approach will have to be adjusted and refined in realistic cases. We plan to use two different events, adopting a retrospective approach. Evaluation through retrospective studies ensures a high degree of realism and objectivity once appropriate actions for an objective and complete collection of information about the past events have been taken (Leveson, 2001).

The first event will be the runaway incursion of Milano Linate, one of the most severe ATM related accidents that occurred in Europe in the last decade. The Milano Linate accident happened in 2001 when a departing MD-87 collided with a Cessna 525-A, which taxied onto the runway. All 114 occupants of the two aircrafts were killed along with four ground staff. The Cessna's crew crossed by mistake the active runway under low visibility conditions, the ATM system was unable to support the crew adequately and to tolerate their mistake (Agenzia Nazionale per la Sicurezza del Volo, 2004).

The second case was an incident that occurred in 2005, when severe weather conditions obliged a B737 aircraft to divert from its original destination airport of Ciampino to Fiumicino and then to Pescara. The aircraft violated altitude restrictions in Fiumicino. Crew operations were in an area of intense traffic. Technical constraints in the ATM system contributed to deficiencies in the insurance of adequate traffic management services. The incident had no consequences for humans or goods (Agenzia Nazionale per la Sicurezza del Volo, 2009).

The two events have several aspects in common that make them suitable for a comparative analysis. Both happened in severe weather conditions combined with operational, technical and organizational factors. Contributing factors were workload, safety nets missing or out of service and communication issues. In both of them the ATM system (managed by the same service provider) had a major role. However, there were also substantial differences that in one case led the ATM system to the inability to adapt and tolerate the negative situation, while in the other to still ensure adequate traffic management services. We intend to apply the SCALES framework in the two case studies, identifying the key indicators that should quantify the resilience of the ATM system, and their values and evolution till the events. We also plan to identify and measure the early warning signs that should have indicated the likely system degradation.

The idea is to apply SCALES to the story of everyday successful operation and the stories that led to these two events. The mapping in EA will allow system of systems consideration of operational, contextual and organizational conditions. The RE analysis will allow to identify relevant indicator candidates and measure these in those events. We will include a predefined period before those events (e.g. 12 and 6 months prior to the event and right before the event). These data will allow identification and evaluation of relevance of these indicators and to measure the potential for resilience; quantitatively and qualitatively. We would like to see how the indicators evolve over time and are used by the organizations. Furthermore, we will analyse if some indicators can be seen as early warnings for system degradation. SCALES and indicator candidates will be discussed in workshops with operational and organizational aviation personal to have a consensus on the most appropriate indicators for these cases.

3 EVALUATION

Using the retrospective studies we will be in condition to apply and validate the SCALES approach in realistic conditions evaluating the following functional characteristics:

1) Ability to identify quantitative and qualitative set of indicators that are representative of the system resilience before and up to the events of the case studies;

2) Ability to identify early warning signs for likely system degradation and

3) Ability to show significant trends of indicators and early warning signs before and up to the events of the case studies.

In addition, the case studies will allow evaluating quality characteristics of the SCALES framework. These are reported in Table 1 including how the evaluation is performed.

Table 1 Validation criteria to evaluate SCALES framework

Characteristic	Explanation of the quality characteristic	How to evaluate
Applicability	Check if the SCALES framework is reasonably easy to use and understand	Practical use in the case studies
Reliability	Check if results are credible and correct, and if there are reasonable confidence margins	Comparison of SCALES vs. real outcome of the events
Cost effectiveness	Check if the application effort required and associated costs are acceptable	Expert judgement
Scalability	Check if the SCALES approach can be used with systems of higher complexity with a reasonable increase in cost and workload while maintaining its quality characteristic	Practical use in the case studies and theoretical evaluation of its applicability to larger systems

4 DISCUSSION AND CONCLUSIONS

In complex socio-technical system like ATM, we plan to address how the system adapts to continue operation focusing on the identification of resilience related indicators. The trade-offs can provide the theoretical basis to produce metrics in this context (Hoffman and Woods, 2011). SCALES will address the five fundamental trade-offs as follows:

- Optimality-Resilience of Adaptive Capacity Trade-Off: Indicators related to the capacity to adapt (**respond**), to identify degradation (**early warnings**) and **anticipation** of resources needed to cope with situations.
- Effciency-Thoroughness Trade-Off: EA enables the representation of the work as performed, including procedures and practices. Indicators related to the **flexibility** of these procedures and ability to put and update plans in practice are explored (**anticipate and learn**).
- Revelation-Reflection on Perspectives Trade-off: EA enables **different view points** on the system stimulating to identify indicators related to cross-scale interactions within and across systems-organizations.
- Acute-Chronic Goal Responsibility Trade-Off: Indicators related to management and prioritizing of **roles and responsibilities** within and across organizations when addressing conflicting goals.
- Concentrated-Distributed Action Trade-Off: Indicators related to quality of **coordination of activities within and across organizations**.

The ATM system is characterized by dynamic interactions among different aviation stakeholders. Each actor focus its adaptation to their priorities, to analyze the system it would be necessary to see the combined interactions to determine the effect of the interaction and the manage of trade-offs (time pressure, resources, collaboration within and across organizations). Existing approaches for safety analyses apply decomposition. We build upon a system of systems approach modeling of interaction and adaptations via Enterprise Architecture. The main result from the project will be the SCALES framework. In addition, we aim to produce the following results:

- Advances in theory: by combining the fields of Enterprise Architecture and Resilience Engineering to provide more efficient and more confidence of the representativeness of the indicators.
- Advances on practical representations of resilience analysis including a questionnaire. Currently resilience analysis lack of the use of advanced tools that support Resilience Engineering.
- Promote and facilitate use of enterprise architecture and resilience engineering: Verification and validation in realistic cases representing highly relevant technical and operational functions and typical for future ATM.

The expected benefit of combining an EA with RE is two-fold. *Firstly*, SCALES will apply principles from EA in order to get a good system of systems overview ATM system and

from RE to support the identification of the related logical, organizational and technological resilience related indicators. *Secondly*, after having validated and refined the initial SCALES framework in a case study consisting of two real incidents (reference) the resulting SCALES framework will, accompanied by a set of guidelines, demonstrate how resilience related indicators can be identified and measured using different viewpoints of a system and be made available for others to use via an accessible and user-friendly web interface.

This paper presents the preliminary ideas to combine EA and RE, further work is needed in the detail specification of questions and application of the SCALES framework in the case studies. We invite the Resilience Engineering community to provide a feedback on the method and ideas presented in this paper.

ACKNOWLEDGEMENTS

The work planned in SCALES will be partly funded of the SESAR WP-E Programme on long-term and innovative research in ATM. Disclaimer: this paper presents autors view.

REFERENCES

Agenzia Nazionale per la Sicurezza del Volo (2004). Milano Linate Aerodrome after collision between SK686 and D-IEVX, Audit Report.

Agenzia Nazionale per la Sicurezza del Volo (2009). Inconveniente grave occorso all'aeromobile B737-800, marche EI-DAV, Rapporto d'inchiesta.

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science*, *37*, 109-126.

Hoffman, R.R., Woods, D.D. (2011). Beyond Simon's Slice: Five Fundamental Trade-Offs

that Bound the Performance of Macro cognitive Work Systems. IEEE.

Hollnagel, E. (2009). The four cornerstones of resilience engineering. *Resilience Engineering Perspectives, vol. 2, Preparation and Restoration*. Ashgate, Aldershot, UK.

Hollnagel, E., Leveson, N., Woods, D. (2006). Resilience Engineering Concepts and Precepts, Aldershoot: Ashgate (*)

Leveson, N. (2001). Evaluating accident models using recent airspace accidents.

Leveson, N. (2004). A New Accident Model for Engineering Safer Systems. *Safety Science 42*, 237-270

Reiman, T., Pietikäinen, E. (2010). *Indicators of safety culture. Selection and utilization of leading safety performance indicators*. Research Report 2010:07.

Westerheim, H., Natvig, M. (2004). Functional decomposition based on the ARKTRANS reference model, Procs of Moving towards an integrated Europe. Budapest, Hungary.

Woods, D. (2006). Essential Characteristics of Resilience (*)

Wreathall, J. (2006). Property of Resilient Organization: An Initial View (*)