Resilience in ATM operations: Incorporating Robustness and Resilience in Safety Assessment

Rogier Woltjer[1], Jonas Haraldsson[1], Ella Pinska-Chauvin[2],
Tom Laursen[3], Billy Josefsson[4]
[1] Swedish Defence Research Agency, Linköping, Sweden
rogier.woltjer@foi.se, jonas.haraldsson@foi.se
[2] EUROCONTROL, Brétigny-sur-Orge, France
ella.pinska-chauvin@eurocontrol.int
[3] IFATCA & NAVIAIR, Denmark
mettom@private.dk
[4] NORACON/LFV, Norrköping, Sweden
billy.josefsson@lfv.se

Abstract. The paper describes the approach taken to analyse air traffic operations and develop robustness and resilience guidance, with a focus on resilience. It summarizes the main principles of robustness and resilience applied to ATC/ATM as developed in the SESAR JU 16.01.02 project. The on-going project aims to incorporate these principles as part of safety assessment guidance into the SESAR Safety Reference Material and formulate the principles for ATM concept design. Specifically, the following resilience aspects are discussed in detail: actual practice, procedures and techniques of all actors, goal trade-offs, adaptive capacity, human performance, capacity near margins, buffers and tolerances, coordination, complexity, coupling, interactions, tractability, cascading, control time scales, timing, pacing, and synchronization, under-specification and approximate adjustments. Operational examples to illustrate some of these principles are provided.

1 INTRODUCTION

Air Traffic Management (ATM) safety is usually addressed in safety assessment and

design by means of minimizing negative outcomes through attempting to eliminate hazards, preventing adverse events, setting constraints, or protecting/mitigating against adverse consequences. However, considering the actual number of incidents of about one in 10.000 non-incident events, understanding safety cannot be based exclusively on incidents (EUROCONTROL, 2009). Thus, new perspectives focusing on understanding everyday operations are necessary. The perspectives of Resilience Engineering (Hollnagel et al., 2006; 2011) and Safety-II (Hollnagel, 2012a) aim to understand why everyday performance succeeds. In this context, safety is understood as the ability to succeed under varying conditions (Hollnagel, 2011b).

As part of the Single European Sky (SES) initiative of the European Commission, the SESAR (Single European Sky ATM Research, see www.sesarju.eu) programme is designing new ATM concepts with the aims of improving fuel efficiency, cost efficiency, safety, and airspace capacity. A large number of technical and operational projects aim to develop concepts (technology and working methods) towards these goals, meaning that new trade-offs between safety, efficiency, and capacity will likely need to be found for future operations. Functional changes and new trade-offs have the potential to make socio-technical systems brittle (Hoffman & Woods, 2011; Woods & Branlat, 2011) emphasizing the need for Resilience Engineering and Safety-II concepts in ATM.

The concepts and perspectives from the new Resilience Engineering discipline have as yet hardly made their way into Air Navigation Service Providers (safety) management processes. SESAR Project P16.01.02 "Ensuring ATM with SESAR is kept resilient" described here aims to do a step in that direction. The SESAR Safety Reference Material (SRM) (Fowler, Perrin, & Pierce, 2011) is the process by which operational and technical projects assess safety of the concepts they develop. There are a suite of research projects (e.g., P16.01.02) looking to explore how novel approaches to safety can be delivered into SESAR. Their vehicle to do this is via the SRM, as technical annexes. Thus, P16.01.02 has been assigned by SESAR Joint Undertaking to develop guidance for resilience to be part of the SRM, as well as general resilience design guidelines for ATM.

Based on the resilience literature the following working definition for resilience was derived for the 16.01.02 project. The working definition of robustness was derived from the definition of resilience focusing on anticipation and handling expected disturbances, in its scope closer to a Safety-I (Hollnagel, 2012a) approach.

Robustness is the ability of the ATM system to anticipate and handle expected disturbances, whilst sustaining required operations.

Resilience is the ability of the ATM 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, 2011b, p. xxxvi).

A two-fold approach was chosen for this study with robustness interpreted as a first step towards the broader and more encompassing emergent property of resilience.

2 METHOD

2.1 Robustness: Incident data

In the initial phase an incident analysis template was developed, for incident analysis from both robustness and resilience perspectives, with a focus on robustness.

The robustness part of the template was developed by simplifying HERA-SMART (Pariès et al., 2003), a method derived from Reason's Swiss Cheese metaphor (Reason, Hollnagel, & Pariès, 2006) adopted to ATM, asking questions on prevention, recovery, and mitigation, regarding events in the incidents. The analysis took place during two one-week workshops involving staff from the Air Navigation Service Providers (ANSPs) utilizing their knowledge of the operational environment where the data were collected from. This analysis included 15 incidents from two European ANSPs and was used to develop Robustness Principles for ATM.

2.2 Resilience: Everyday operations data

As the second stage of the project a series of observations, interviews and workshops addressing everyday operations at Air Traffic Service Units were conducted with a focus on resilience. Observations were focused on 3 operational units (control towers) with a diverse mix of traffic types. Workshops and interviews were conducted with air traffic controllers, managers, and safety personnel from several other towers, area control centres, and terminal area control units, as well as ANSP headquarters. Data was gathered and analysed using concepts described in the emerging Resilience Engineering literature (e.g., Hoffman & Woods, 2011; Hollnagel, 2004; 2009; 2011a; 2011b; 2012a; 2012b; Hollnagel et al., 2006; 2011), and Resilience Principles for ATM were developed.

The resilience part of the incident analysis template (see Section 2.1) was developed by including selected questions from the newly proposed Resilience Engineering method Resilience Assessment Grid (RAG; Hollnagel, 2011a) as well as other questions derived from the Resilience Engineering literature. The resilience analysis of the incidents was included in the generation of the Resilience Principles.

3 RESULTS

3.1 Robustness Principles

The Robustness Principles include the following subjects:

- varying conditions,
- actual practice, procedures and techniques,
- signals and cues,
- technical transparency,
- predictability, usability,
- human performance,
- control time scales,
- controlling practice or "defensive" controlling,

- communication aspects,
- ATC-cockpit interactions,
- stepwise implementation,
- airspace/airport design,
- automation.

There are similarities and links between the Robustness and Resilience Principles, due to the project approach of using robustness as a first step towards resilience. Robustness and Resilience Guidance merged towards the end of the project. The focus of the remainder of this paper is on the Resilience Principles for ATM.

3.2 Resilience Principles

The Resilience Principles (numbered ResP*nn*) include the following subjects:

- actual practice, procedures and techniques of all actors,
- goal trade-offs,
- adaptive capacity,
- human performance,
- capacity near margins, buffers and tolerances,
- coordination,
- complexity, coupling, interactions, tractability, cascading,
- control time scales,
- timing, pacing, and synchronization,
- under-specification and approximate adjustments.

ResP01: Actual practice, procedures and techniques of all actors. Safety assessments should be sensitive to actual everyday operator performance, and to specific conditions of operational environments and tools, and how these interact with each other and with ATM changes. Rather than labelling these as “human errors” or “deviations” from procedures or training, Resilience Engineering aims to gain a deeper understanding and appreciation of performance variability (Hollnagel, 2004). This includes operators’ techniques to handle situations beyond what is addressed in procedures or training. With operators we mean not only controllers but also stakeholder and actors (in)directly interacting with ATC, including pilots, airline operations centres, ground vehicle operators, maintenance personnel, military airspace users, etc. “Techniques” refer to the ways operators use procedures and other working methods, strategies and practices to achieve safety and efficiency.

ResP02: Goal trade-offs. The recognition of the effects of multiple goals is critical for understanding the variability that arises in daily operations (see Hollnagel, 2009; Hoffman & Woods, 2011). In SESAR terms, Key Performance Areas (KPAs) such as Safety, Security, Environmental Sustainability, Cost Effectiveness, Capacity, Efficiency, Flexibility, and Predictability are often tightly coupled and related in that optimising or prioritising one may affect others. In that sense a design of an operational ATM functional system is by necessity sacrificing all KPAs to some extent, and some more than others. Furthermore one may identify conflicts within and between these KPAs, such as long-term versus short term goals, goals from different functional systems or

stakeholders' perspectives (e.g. ANSPs versus other actors on and around the airport). Anticipating how a design and its associated operational performance can strike an appropriate trade-off is essential from a Resilience Engineering perspective.

Example 1: Techniques & trade-offs. Capacity goals may have been optimized and set in a manner to satisfy safety goals, while leaving little margin for variations in behaviour. For example, the capacity for landings per hour may be set to a certain (high) number meaning that in peak traffic hours the traffic has to be separated at the minimum separation (and exceptions may have been approved that enable separating below the standard separation, further decreasing margins). Ways of performing the function Sequencing & Spacing to meet these capacity goals may be highly reliant on physical solutions (e.g. high speed runway exits) and predictability in conditions (e.g. visibility, winds), possibilities of controlling traffic (e.g. actively controlling approach speed of aircraft, which makes the performance of the approach more brittle from a pilot's perspective) and skill (controllers having developed techniques through training and experience on safely controlling with little margin).

Example 2: Techniques & trade-offs. APP controllers performing the function Sequencing & Spacing, may be currently doing radar vectoring from the feeder fix to runway threshold in order to take into account unexpected flights entering the sequence late, avoid adverse weather (e.g., CB), vector other traffic around unexpected aircraft movements, handle emergencies, etc., while maintaining a high runway capacity and high service level for airspace users. How this vectoring is done is a technique not specified in detail in the procedures. Change of new scheduling concepts and technology using for example points further or closer from the threshold or at the threshold, would change the ability for the ATM system to provide the Sequencing & Spacing function flexibly and effectively, and would change the ability to handle unexpected events. This technique therefore needs to be considered when making AMAN scheduling changes and thereby changing the Sequencing & Spacing function in the TMA.

ResP03: Adaptive capacity**.** The effects of many conditions can to a certain extent be anticipated analytically or through simulation, and mitigated as part of design, development and safety assessment. This preparation forms the *base* adaptive capacity of the ATM functional system, including training, procedures, HMI and technical capabilities, and degraded modes and contingency plans. The Resilience Engineering perspective recognises that one will (as a consequence of complexity and dynamics) never be able to go through the full range of possible operational scenarios that will occur during the operational lifetime of a technical system, operational concept, or ATM unit. Unexpected events will occur at some point, which don't quite match the conditions for triggering the planned responses. Adjustments, adaptations, flexibility, and/or improvisation are necessary to a varying degree, based on experience (see also Hollnagel, 2009; Woods & Branlat, 2011).

ResP04: Human performance. Most of the adaptive capacity that goes beyond the base adaptive capacity of the ATM functional system is based on operators' exclusively

human capabilities (especially attention management, problem detection, adaptation to situational circumstances, ability to achieve goals using different means and methods). This human (or team) ability of providing resilience can only be preserved if the conditions and information necessary for operators to be in control and adapt (through processes of anticipating, monitoring, and responding) are acknowledged.

ResP05: Buffering capacity near margins, and tolerance. In order to meet the challenges of the inescapable nature of unexpected events and adjusting the base and beyond-base adaptive capacity, several characteristics of resilient systems can be engineered into the functional system to improve the ability to anticipate when the system should adapt and providing it with a readiness to respond and meet changing demands before hazardous situations occur. Several such systemic characteristics have been identified, such as buffering capacity, margins, tolerance, and flexibility (Woods, 2006).

Example 3: Margins. Alternate airports and fuel levels and margins seem to be handled differently today by flight crews and airlines than some years ago. Functional changes to the ATM system (e.g. tools and working methods) that pertain to approach should acknowledge the way flight crews handle fuel margins and in various circumstances.

ResP06: Coordination. The ability to flexibly coordinate between ATCOs, pilots, and all other actors and stakeholders when the situation demands this is a major source of resilience that needs to be addressed explicitly in safety assessment for ATM changes. Human operators rely to a significant extent on flexible and improvised use of coordination and communication content (what is said) and channels (who to contact and how) in order to solve challenging situations that go beyond the base adaptive capacity to handle varying conditions. Technology-based functional changes such as automated communication and information sharing will thus likely affect the ability to cope with unexpected challenges and disruptions, which need to be assessed.

ResP07: Complexity, coupling, interactions, tractability, cascading. Central to Resilience Engineering for ATM is an understanding that the ATM functional system should be regarded as a network of nodes where functions are performed in a distributed manner. Properties (cf. KPAs) such as efficiency, capacity, flexibility, safety, and resilience are dynamic and cannot be attributed to static properties of components but emerge out of the joint behaviour of the nodes in a distributed air traffic system. More complexity and less tractability typically lead to higher demands on human operators and human-technology-systems in unanticipated situations, and typically increase the risk for small variations cascading (unpredicted and undetected) into hazardous situations, resulting in a more brittle (less resilient) system.

Example 4. Complexity and tractability. In one of the incidents studied, an inactivated flight was manually activated in an unexpected manner (the activation looked solved for that ATCO and sector perspective). The flight activation however was sent to the previous rather than the next sector. Underlying technical system logic turned out to be incompatible with actual ATCO problem solving methods leading to a brittle system.

ResP08: Control time scales. Critical aspects of resilience are the timing aspects of synchronisation and the pacing of tasks. Effects at different time scales should be considered in assessing resilience as for example carry-over effects from strategic to pre-tactical to tactical operations across various stakeholders as they may cascade into non-linear effects (see also Woods, 2006).

ResP09: Timing, pacing, and synchronization. The dynamics of the ATM system are critical to understand when assessing which aspects of a change make the functional system resilient and which make it brittle, especially in human-automation joint systems (DSB, 2012). Time may in many cases be the aspect providing buffer capacity.

ResP10: Under-specification and approximate adjustments**.** Under-specification means that descriptions of procedures and the use of technical systems are not fully specified for the actual situations that will be met during everyday operations, because the conditions of work cannot be fully specified. Thus operators necessarily have to make approximate adjustments of their performance to the context, and their performance has to be variable, to be able to cope with unexpected situations and conditions (Hollnagel, 2004, 2009, 2012b). From a safety assessment perspective it should be recognized and anticipated to the highest extent possible that SOPs and tools will be used in different ways than exactly as-designed, to meet varying demands.

4 CONCLUSIONS

The paper describes the approach taken to analyse air traffic operations and develop robustness and resilience guidance, with a focus on resilience. It summarizes the main principles of robustness and resilience applied to ATC/ATM as developed in the SESAR JU 16.01.02 project. Operational examples to illustrate some of these principles have been provided.

Based on these principles, preliminary SRM Robustness and Resilience Guidance has been derived. On-going continuation of this development includes validation of the guidance on SESAR R&D projects and refining the guidance to fit into the SRM, as well as validating the principles as design guidelines for ATM. Ideas for future research in the ATM industry include extending the Safety-II and Resilience Engineering approach into ATM management beyond the established safety assessment and human performance assessment processes.

ACKNOWLEDGMENT

The project work presented in this paper is part of the SESAR Joint Undertaking P16.01.02 and we gratefully acknowledge the contribution of project-external informants and the project members from the SJU P16.01.02 project partners: NORACON, EUROCONTROL, NATS, AENA, ENAV, INDRA, and AIRBUS. Opinions in this publication are the authors' and are not intended to represent the positions of SESAR JU or its project member organisations.

REFERENCES

DSB. (2012). *Defense Science Board Task Force Report: The Role of Autonomy in DoD Systems*. Washington, DC, USA: DoD.

EUROCONTROL. (2009). *White Paper on Resilience Engineering for ATM*.

Fowler, D., Perrin, E., & Pierce, R. (2011). 2020 Foresight - a Systems-engineering Approach to Assessing the Safety of the SESAR Operational Concept. *Air Traffic Control Quarterly, 19*(4), 239–267.

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

Hollnagel, E. (2004). *Barriers and accident prevention*. Aldershot, UK: Ashgate.

Hollnagel, E. (2009). *The ETTO principle: efficiency-thoroughness trade-off*. Aldershot, UK: Ashgate.

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

Hollnagel, E. (2011b). Prologue: The scope of resilience engineering. In Hollnagel, E., Pariès, J. Woods, D. D., & Wreathall, J. (Eds.) *Resilience Engineering in Practice: A Guidebook* (pp. xxix–xxxix). Aldershot, UK: Ashgate.

Hollnagel, E. (2012a). *A Tale of Two Safeties (Draft)*. Retrieved on 04FEB2013 from http://www.erikhollnagel.com/A_tale_of_two_safeties.pdf .

Hollnagel, E. (2012b). *FRAM: The Functional Resonance Analysis Method - Modelling Complex Socio-technical Systems*. 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., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

Pariès, J., Bieder, C., Reason, J., & Isaac, A. (2003). *The Development of a Safety Management Tool within ATM (HERA-SMART)*. HRS/HSP-002-REP-08. EUROCONTROL.

Reason, J. T., Hollnagel, E., & Pariès, J. (2006). *Revisiting the "Swiss Cheese" model of accidents.* EEC Note No. 13/06. EUROCONTROL.

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