Resilience Engineering in Air Traffic Management

Increasing Resilience through Safety Assessment in SESAR

Rogier Woltjer
Division of Information and Aeronautical Systems
Swedish Defence Research Agency FOI
Linköping, Sweden
rogier.woltjer@foi.se

Ella Pinska-Chauvin
SESAR & Research - Performance & Method Unit
EUROCONTROL
Brétigny-sur-Orge, France
ella.pinska-chauvin@eurocontrol.int

Tom Laursen
IFATCA & Naviair
Denmark
mettom@private.dk

Billy Josefsson
Project Management and Support
NORACON / LFV Air Navigation Services of Sweden
Norrköping, Sweden
billy.josefsson@lfv.se

***Abstract*— This paper describes the approach taken to develop resilience engineering guidance for safety assessment of functional changes in air traffic management (ATM). It summarizes the process of deriving resilience principles for ATM, originating from resilience engineering concepts and transposed into ATC operations. These principles are the foundation for a method incorporating resilience engineering into safety assessment methodology (specifically the SESAR Safety Reference Material), and for providing guidance for various ATM design processes. The methodology was validated via a test case on the i4D/CTA concept. Operational examples from the application of the developed guidance to the i4D/CTA concept are provided. Initial evaluation of the guidance suggests that it 1) surfaces new issues not addressed explicitly in safety assessments or project discussions; 2) is less formal and more qualitative than traditional methods and brings the discussions of these issues closer to operational practice; and 3) provides a vocabulary and documentation means of project discussions on resilience not currently documented. The guidance thus seems to facilitate an interweaving and systemic integration of operational, management, safety, and human performance aspects, while enriching the description and assessment of emergent properties and functional changes in ATM.**

Keywords: resilience; resilience engineering; air traffic control; air traffic management; safety assessment; safety-II

I. 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, but should attempt to understand all outcomes (positive and negative) of everyday operations [1], [2]. Thus, new perspectives focusing on understanding everyday operations are necessary. The perspectives of Resilience Engineering [1], [3], [4] and Safety-II [2] aim to understand why everyday performance succeeds. In this context, safety is understood as the ability to succeed under varying conditions [5]. Varying conditions are always under-specified. Individuals and organizations must therefore adjust what they do to match current demands and resources. Because resources and time are finite, such adjustments will inevitably be approximate. Performance variability is defined as the ways in which individual and collective performances are adjusted to match current demands and resources. Performance variability and approximate adjustments by the ATM/ANS functional system are necessary, inevitable, and useful, and the reason why everyday work is safe and effective, but at the same time they can play a role in why unexpected or undesired outcomes occur. Unexpected outcomes can result from everyday processes that interact in unexpected ways. Thus, all outcomes are due to performance variability and approximate adjustments. Categorizations of outcomes (such as positive/negative, success/failure) are judgments of value rather than objective binary categories.

As part of the Single European Sky (SES) initiative of the European Commission, the SESAR (Single European Sky ATM Research, see www.sesarju.eu) program 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 [6], [7], emphasizing the need for Resilience Engineering and Safety-II concepts in ATM.

The project work presented in this paper is part of the SESAR Joint Undertaking project P16.01.02.

Adopting this view creates a need for an approach that can represent the everyday performance variability and emergent properties of ANS/ATM functional systems. Emergent properties are properties of the ANS/ATM system that arise at higher levels of complexity out of relatively simple processes or interactions, and are the result of system components and processes (people, procedures, equipment) working together or impacting each other. Resilience Engineering attempts to understand and manage performance variability and address safety, efficiency, and resilience as emergent properties.

Resilience Engineering for ATM requires an integrated approach to anticipation, monitoring, response, and learning [5], [8]. Applying the Resilience Engineering principles fully would therefore impact many aspects and processes of ATM operations and aviation safety and business management. The scope of the present Guidance Material is however restricted to safety assessment as per SESAR V1-V2-V3 development phases (Scope, Feasibility, Pre-industrial development and integration) and the SESAR Safety Reference Material (SRM).

The concepts and perspectives from the new Resilience Engineering discipline have as yet hardly made their way into Air Navigation Service Providers safety or business 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) [9] 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 (SJU) to develop guidance for resilience to be part of the SRM, as well as general resilience design guidelines for ATM.

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." ([5], p. xxxvi). The project set out to apply this definition to the ATM/ANS functional (people-procedures-equipment) system. Note that since this definition includes expected conditions, which is the focus of traditional methods within the Safety-I paradigm, there is a complementary relationship of traditional methods and perspectives and the resilience/Safety-II perspective [2], which is also reflected and explored in this project.

Note that this definition includes expected conditions, which is the focus of traditional methods within the Safety-I paradigm. There is a complementary relationship of traditional methods and perspectives and the resilience/Safety-II perspective [2], which is also reflected and explored in this project.

Section II of this paper describes the method of the project of analyzing incidents, everyday operations, development of resilience guidance and application to a case. Section III describes the project results in terms of Resilience Principles to be considered in safety assessment and design guidance. Section IV provides a short discussion and conclusion.

II. METHOD

A. *Incident Analysis*

The project adopted a gradual approach to transitioning from Safety-I to Safety-II concepts and methods, in order to connect the resilience approach to current industry vocabulary and illustrate a resilience perspective of explaining past events. Incidents from a resilience engineering perspective are due to the same performance variability that is necessary in everyday operations to adapt to varying conditions. Incidents can thus be used to derive information about everyday adjustments. Safety-II should be able to explain performance variability and all of its outcomes (traditionally labeled positive and negative). The initial phase of the project therefore adopted an approach of applying both Safety-I and II perspectives on a series of incidents, to shed light on the everyday adaptations related to these incidents.

In the initial phase an incident analysis template was developed, by simplifying HERA-SMART [10], a method derived from Reason's Swiss Cheese metaphor [11] 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 environments that the data were collected from. This extensive analysis included 15 incidents from two European ANSPs. The resilience/Safety-II 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) [8] as well as other questions derived from the Resilience Engineering literature.

B. *Everyday Operations Analysis*

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 centers, and terminal area control units, as well as ANSP headquarters. Data was gathered and analyzed using concepts described in the emerging Resilience Engineering literature [2], [4]–[6], [8], [12]–[14], and Resilience Principles for ATM were developed.

In this way, concepts from the Resilience Engineering literature were attempted to be applied to the study of everyday operations, to evaluate which of these concepts made sense to operational, technical, and safety experts in order to describe properties of the ATM system that make it resilient. It was thus the SJU assignment and aim of P16.01.02 to apply and evaluate

concepts from resilience engineering literature, not to construct a bottom-up analysis and description of everyday operations and ATM resilience. The principles outlined in Section III provide references to the resilience concepts used.

C. Development and Application of Resilience Guidance

As part of the project, Resilience Guidance for safety assessment has been developed, based on the incident and everyday operations analyses described above. The guidance takes the form of questions to ask during the safety assessment of new people-procedure-equipment (functional) changes in ATM. The purpose within this project is for the Resilience Guidance to provide input to the safety assessment according to the SESAR Safety Reference Material SRM. This input is intended to take the form of modifications or additions to the safety objectives, safety requirements, assumptions, issues, validation needs, and/or scenario input (see [9]).

Preliminary Resilience Guidance was applied to two R&D projects within the SESAR JU program. One of these was the i4D/CTA concept. The guidance was applied in a workshop format where everyday operational practice was the backbone of discussions. First, everyday operational practice as currently performed, in terms of delivered services broadly related to the change (e.g., separation management, sequencing and metering, etc.) was described. Second, everyday operational practice in terms of delivered services as envisioned with the (i4D/CTA) functional change was described. Subsequently, using these descriptions, the remaining resilience principles and guidance questions were applied to the change, again in relation to services as currently performed and as envisioned with the change.

D. i4D/CTA Case Description

The i4D/CTA concept is briefly outlined below (see [15] for an early public description of 4D trajectory management). The i4D/CTA concept puts forward 4D trajectory management for improved pre-sequencing purposes. The concept also introduces a higher level of flight crew autonomy.

The i4D concept is used to establish a CTA (Controlled Time of Arrival) through a process of interactions, including establishing data link connection, exchanging weather updates, 2D flight plan and 3D route agreement, performance profile and estimated arrival time window communication.

With the CTA, a metering fix about 40 NM before the runway threshold is set in the TMA (terminal maneuvering area). The CTA is suggested by extended AMAN (Arrival MANager) software based on the estimated time of arrival downlinked by the i4D aircraft, and accepted or rejected by the en-route air traffic controller.

From the aircraft perspective, a CTA is flown through flight management system operation as an RTA (Requested Time of Arrival at a given waypoint).

The benefit for airlines is that the aircraft flies more self-managed to the metering fix, thus flying optimally from the perspective of energy (fuel) management, and that other stakeholders gain more accurate estimated landing times.

It should be noted that the i4D/CTA concept is under development and that the 16.01.02 project and therefore the current paper cannot and do not aim to conclusively evaluate the i4D/CTA concept as such. The present paper merely aims to illustrate the resilience principles using the i4D/CTA concept as a case, and to discuss some of the changes that come with introducing this new concept (as far as development has come thus far), in dialogue with projects that develop i4D/CTA.

III. Results

The Principles for the assessment of resilience include the following subjects:

- work-as-done,
- varying conditions,
- signals and cues (anticipation, monitoring, response),
- goal trade-offs,
- adaptive capacity,
- coupling and interactions,
- timing, pacing, and synchronization,
- under-specification and approximate adjustments.

The focus of the remainder of this paper is to present the Resilience Principles for ATM and give examples of the application of our Resilience Guidance to the i4D/CTA concept.

A. Work-as-done

Resilience Engineering aims to gain a deeper understanding and appreciation of performance variability. This includes understanding work-as-done: operators' techniques to handle situations addressed in procedures or training and beyond. Changes in work-as-done of all relevant stakeholders' operators need to be described and assessed in safety assessment. This starts with a description of work-as-done by establishing an understanding of operators' actual performance and practices, procedures and techniques. This includes, for example, identifying where there are gaps and inconsistencies in procedures and how these are solved, and understanding techniques for meeting possibly conflicting performance goals. With techniques we mean the ways operators use procedures and other working methods, strategies and practices to achieve safety and efficiency. With operators we mean not only controllers but also other actors such as supervisors, technicians, pilots, ground vehicle operators, etc.

Example 1: Actual practice regarding i4D/CTA

Practices of how to control aircraft in en-route and approach phases are affected by i4D/CTA. Two changes that are addressed here are extended AMAN and controller

monitoring of CTAs. Currently the use of AMAN is flexible, as it is a recommendation (e.g. suggested sequence), it is used as information (e.g. for delays) only. The i4D/CTA concept implies an agreement on a 3D trajectory and a Controlled Time of Arrival at the metering fix.

With i4D/CTA, the aircraft flight management system chooses time to loose and gain after manufacturer- and airline-specified profile, which entails more monitoring because of different profiles. A difference in techniques is that rather than controlling aircraft and maintaining separation by clearances along the entire en-route and approach phases, controllers with i4D/CTA will know exactly when to expect aircraft to be at the metering fix, but will not know which descent profile it is going to fly to get there. After CTA acceptance controllers will need to employ a different kind of monitoring of descent profiles, because controllers will not know aircraft top of descent. Even if there is an agreement on 3D trajectory, there is variability of the FMS to adjust speed, rate of descent, etc.

B. Varying conditions

The impact on the ANS/ATM functional system to cope with varying conditions needs to be identified for the affected services/functions and ranges of conditions. Varying conditions includes what can be considered expected and unexpected conditions.

Conditions that have been anticipated, analyzed or modelled, and mitigated, using various engineering and mathematical means can be considered expected conditions. Therefore (in SRM terms) these include normal conditions, abnormal conditions, and failure.

Conditions that were not anticipated or not mitigated (e.g., due to very low probability), may be considered unexpected conditions. This may include combinations of expected conditions.

Expected and unexpected conditions are addressed here under the term varying conditions, without the need to define and distinguish between expected and unexpected as separate binary categories. Responses to unexpected conditions can make use of preparations for expected conditions. Coping with everyday situations relies heavily on operators' ability to use and combine previous experience and preparations for expected conditions (addressed through design features, training, procedures, etc.) in new ways.

For the assessment of varying conditions in various categories guidance was based on a categorization from the threat list of the Normal Operations Safety Survey [15]. Guiding overarching categories may be considered: ANSP conditions (concerning "own" and "other" ANSP services) such as equipment and workspace conditions (including common issues [16] of (un-)serviceability and degraded modes), controller/flight data conditions (e.g., coordination, flight progress strip, and flight plan issues), and operational performance conditions (e.g., unclear procedures, non-standard levels, runway usage issues); airborne, traffic, and pilot-ATC communication issues; and environmental issues (weather, geography, airspace/airport design). The assessment should address both conditions for units that are part of the intended functional ATM change, and units that in some way interact with these but are not part of the change.

Varying conditions may also be assessed using variability modes (e.g., timing, frequency, distance, speed/rate, direction, etc. [12], [14], [17]) that may be linked to a methodological walk-through using various modeling methods.

Lastly, ranges of potentially expected conditions, rather than an estimated typical set of operational environment conditions, needs to be included in the safety assessment from a resilience perspective, as everyday variations in conditions in various European operational units are critical in assessing the impact of a functional change from a Resilience Engineering perspective.

C. Signals and cues (anticipation, monitoring, response)

Signals and cues alert and inform operational staff and are key for successful anticipation, monitoring, and response to varying conditions. Operators need to access, attend, and interpret such information and this information can be parameterized in terms of; information source, content, channel, and timing.

Greater transparency, predictability and flexibility in technology improve operators' abilities to monitor, anticipate and respond. This infers that safety assessment should ensure: Transparent system behavior delivered to operational staff at the HMI; Predictability of automation & what the automation is trying to achieve; System logic that is intuitive to the users, and; Flexibility to allow controllers to control the behavior of technology.

D. Goal trade-offs

ATM has to operate within a dynamic environment of multiple shifting goals. The recognition of the effects of multiple goals is critical for understanding the variability that arises in daily operations (see [6], [13]). 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 optimizing or prioritizing one may affect 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).

A functional change will impact on the ability of the ATM system, and within that the operators, to meet the dynamic goals of the operational environment. Anticipating how a design and its associated operational performance can strike an appropriate trade-off is essential from a Resilience Engineering perspective. Poorly considered trade-offs at the design stage will have to be managed in actual operations at a greater "cost" to the operators, and thus an increase in variability.

EXAMPLE 2: TRADE-OFFS REGARDING I4D/CTA

One trade-off that changes with the change to i4D/CTA is that there is less flexibility for controllers but more predictability for airlines and airport services.

Moreover, the trade-off between operator (controller and pilot) workload on the one hand, and efficiency and capacity of approaches on the other, changes with i4D/CTA. If for whatever reason a gap (e.g. weather changes) in the sequence appears, giving an aircraft more direct routing to fill the gap (as is currently done) may mean that the following aircraft have to implement new CTA proposals increasing workload for controllers and pilots. Thus the flexibility leading to efficiency and capacity gains through controller adaptation (taking an aircraft into a gap and adjusting the sequence) is traded off against workload and predictability in a different way. Another question is if the future i4D/CTA tool can be made to keep up with these changes and to which extent.

E. Adaptive capacity

Adaptive capacity [6], [7] refers to base and beyond-base adaptive capacity, and particularly the information and conditions that enable attention management and problem detection [18], as well as means (technical capabilities, communication, etc.) to achieve immediate goals and to allocate and use additional resources to match unexpected demands.

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 (cf. the discussion on expected conditions above). 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 recognizes 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 [7], [13]) and partly using the preparations in place for expected conditions (comparable to "as a resource" [19]).

Beyond base adaptive capacity is considered to be provided mainly by the human ability (as integral part of the functional system) to dynamically solve problems in an unstable and unpredictable environment, especially through attention management, problem detection, adaptation to situational circumstances, and the ability to achieve and balance goals using different means and methods.

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 [20]:

Buffering capacity [20] regards the size or kinds of disruptions that the ATM functional system can absorb (robustness) or adapt to (resilience) without a major breakdown in service provision. Buffering capacity may be provided by margins, which create the possibility to absorb disturbances, or adaptive capacity, which is a form of adaptation. When buffering capacity through margins and adaptations is exceeded, the tolerance of a system describes how the socio-technical system performs beyond the buffering capacity.

Margin concerns how closely or how precarious the system operates relative to one or another kind of performance boundary [20]; Examples include fuel margins for aircraft operations, airspace margins for not vectoring too close to sector boundaries, time margins in sequencing and spacing activities, and aircraft separation margins.

Tolerance means how a system behaves near a boundary and whether the system gracefully degrades as stress/pressure increase, or collapses quickly when pressure exceeds buffering capacity [20].

Assessments of changes to ATM functional systems need to take these aspects into account from a resilience perspective.

EXAMPLE 3: MARGINS AND I4D/CTA

A question (subject to ongoing evaluation) with regard to performance boundaries is how many CTAs can be handled, where the work of giving CTAs and monitoring them is not worth reduced capacity (at some point there is a boundary that does not outweigh the benefit), also regarding mixed traffic scenarios and fitting non-i4D aircraft into the sequence.

Airspace design (e.g. sector boundaries, metering fixes, planned rate of descent, levels at various points) may shape buffering capacity and tolerances, in that there are implications of the change to accommodate aircraft with various performance profiles (due to aircraft design characteristics or emergency), and to facilitate departures respective to inbounds.

Generally, more optimization to use the runway comes with decreased tolerance and margin. E.g., a tight sequence with set CTAs leaves little margin to manage weather changes or aircraft with an emergency and avoid a knock-on effect of changed CTAs, because the margins were set tight in the first place.

F. Coupling and interactions

Central to Resilience Engineering for ATM is an understanding that the ATM functional system should be regarded as a complex network of nodes where functions are performed in a distributed manner.

Coupling refers to the time-dependency of a process, the flexibility of action sequences, the number of ways to achieve a goal, and the availability of slack in operational resources [21]. Tractability refers to the extent to which the detailed functioning of a dynamic system can be described and understood [2], [22]. Cascading [7] is the extent to which small variations (which are unpredicted and undetected) combine into hazardous situations. Interactions are defined as the number of variables and causal relations in the system's processes and interconnected subsystems [21].

More complex and less tractable systems lead to higher demands on operators and functional ATM/ANS systems. Small variations may have a large effect on safety through propagation and amplification of variability [12], [14] across functional ATM systems.

When undertaking safety assessment, the changes in coupling and interactions and the potential for cascading effects need to be identified and assessed.

EXAMPLE 4: COMPLEXITY, CASCADING, AND I4D/CTA

As pointed out before i4D/CTA will lead to a less flexible sequence, sequencing is based on the assumptions that a/c are sticking to the STAR profile. Any non-standard event may cause a knock-on effect.

The assumption of 30 min flying time in en-route sectors may be questioned as complicated geography, complicated sector boundaries, traffic patterns to/from many airports and TMAs, and use of temporarily restricted areas, may lead to significantly quicker transfers between sectors, not uncommon in e.g. central Europe. This means that cascading of effects of i4D/CTA commitments and diversions from commitments may be difficult to predict.

To benefit from i4D level caps have to be issued long before a sector/FIR boundary that can cause a problem for sectors with mountainous geography or airports with small or complex sectors, depending on airspace design.

Another issue is potential cascading effects of speed variability. Before CTA speed is regulated by FMS, after CTA all aircraft have to be on the same speed in order to have separation, which means that large modifications in speed may be necessary, which has implications for workload on the flight deck, and for the controller and the approach sequence if necessary speed changes are higher than can be achieved.

G. Timing, synchronization, and time scales

The dynamics (including timing, pacing, and synchronization [23]) 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. Aspects that need to be considered in assessments include: How long tasks take for operators in comparison to how much time is available. This is especially true in situations where buffers may have already been eroded, e.g. degraded modes; The point in time at which data and resources in one task need to be available for other functional units; How the continuous pacing and synchronization of interdependent functional units contributes to smooth operations and how mismatches create brittleness; How time might provide margin; The potential for carry-over effects from strategic to pre-tactical to tactical operations across various stakeholders as they may cascade into non-linear effects.

Addressing these points provides for a more in depth understanding of how time contributes to system resilience.

H. 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 [12]–[14]. From a Resilience Engineering perspective on safety assessment it should be recognized and anticipated that the intent of the procedure, and the goals to be achieved with the new tool, need to be central to and transparent in the design of the SOP and tool. It should be recognized that SOPs and tools will be used in different ways than exactly as-designed to meet varying demands and balance operational goals.

EXAMPLE 5: UNDER-SPECIFICATION IN I4D/CTA

As pointed out before there is under-specification in the procedures so that controllers through applying various techniques currently contribute to high flexibility, efficiency, and capacity in sequence management. The i4D/CTA concept will change this human contribution.

There is also under-specification in the procedure for the controller accepting/rejecting CTAs from AMAN, related to the intrinsic under-specification of the AMAN system. Controllers cannot know if the data coming into the AMAN is complete or not, which is why a feasibility check is required. At the moment it is a judgment call to accept the CTA or not. Controllers base the decision of implementing the CTA on the traffic flow and whether there is a point to add another constraint. Thus there are no fixed criteria for determining the feasibility of the CTA, comparable to the judgment today of the AMAN suggested schedule. Information (e.g., weather) is not always known, and there may be a time lag for obtaining it. This decision is thus not easily made into a rigid procedure, as controllers will need to act based on judgment and experience.

IV. CONCLUSIONS AND DISCUSSION

The paper describes the approach taken to analyze air traffic operations and develop resilience assessment guidance. 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 using the i4D/CTA case.

We wish to express some preliminary findings of using the resilience guidance, in our experience thus far. First, it surfaces some new issues that are not addressed explicitly in safety assessments or project discussions. Second, assessment through the resilience guidance evaluated here is less formal and more qualitative than traditional safety-I methods, and brings the discussions of these issues closer to operations, which is easy to relate to by controllers as well as project managers and concept developers. Even in early stages of concept development, and especially when real-time simulations evaluating the concept have been performed, they seem to be able to apply the principles to current and envisaged (after the change) operations during guided application workshops. Third, the resilience guidance therefore also enables the documentation of ongoing discussions in the project by providing a vocabulary about aspects that enable resilience and are recognized as such but not documented explicitly as part of concept development practices. To summarize, the guidance seems to facilitate an interweaving and systemic integration of operational, management, safety, and human performance aspects, while enriching the description and assessment of emergent properties and functional changes in ATM.

On-going continuation of this development includes refining the guidance to fit into the SESAR V-phases design cycle as well as reshaping the resilience guidance into design guidelines for various (technical, airspace, procedure, concept) ATM design roles. 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

We gratefully acknowledge the contribution of informants (especially air traffic controllers, and staff association and airspace user representatives) and project members and safety experts of the i4D/CTA projects, and the SJU P16.01.02 project members and workshop participants from NORACON (especially Michaela Schwarz), EUROCONTROL (especially Nicolas Fota and Andrew Kilner), NATS (especially Jason Cawdron), AENA (especially Miguel Capote Fernandez), ENAV (especially Tiziana Russo), INDRA (especially Luis Santoyo and Carlos Alonso), and AIRBUS (especially Joelle Monso and Eric Hannouz), as well as Jonas Hermelin of FOI. Opinions in this publication are the authors' and are not intended to represent the positions of SESAR JU or its project member organizations.

REFERENCES

[1] EUROCONTROL, "A White Paper on Resilience Engineering for ATM," 2009.

[2] EUROCONTROL, "From Safety-I to Safety-II: A White Paper." 2013.

[3] E. Hollnagel, D. D. Woods, and N. Leveson, Eds., *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate, 2006.

[4] E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, Eds., *Resilience Engineering in Practice: A Guidebook*. Aldershot, UK: Ashgate, 2011.

[5] E. Hollnagel, "Prologue: The scope of resilience engineering," in *Resilience Engineering in Practice: A Guidebook*, 2011, pp. xxix–xxxix.

[6] R. R. Hoffman and D. D. Woods, "Beyond Simon's Slice: Five Fundamental Trade-Offs that Bound the Performance of Macrocognitive Work Systems," *IEEE Intell. Syst.*, vol. 26, no. 6, pp. 67–71, Nov. 2011.

[7] D. D. Woods and M. Branlat, "Basic patterns in how adaptive systems fail," in *Resilience Engineering in Practice: A Guidebook*, E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, Eds. 2011, pp. 127–143.

[8] E. Hollnagel, "Epilogue: RAG – The Resilience Analysis Grid," in *Resilience Engineering in Practice: A Guidebook*, 2011, pp. 275–296.

[9] D. Fowler, E. Perrin, and R. Pierce, "2020 Foresight - a Systems-engineering Approach to Assessing the Safety of the SESAR Operational Concept," *Air Traffic Control Q.*, vol. 19, no. 4, pp. 239–267, 2011.

[10] J. Pariès, C. Bieder, J. Reason, and A. Isaac, "The Development of a Safety Management Tool within ATM (HERA-SMART) (EUROCONTROL HRS/HSP-002-REP-08)," Brussels, 2003.

[11] J. T. Reason, E. Hollnagel, and J. Pariès, "Revisiting the 'Swiss Cheese' model of accidents (EUROCONTROL Experimental Centre EEC Note No. 13/06)," Bretigny-sur-Orge, France, 2006.

[12] E. Hollnagel, *Barriers and accident prevention*. Aldershot, UK: Ashgate, 2004.

[13] E. Hollnagel, *The ETTO Principle: Efficiency-Thoroughness Trade-Off: Why Things that Go Right Sometimes Go Wrong*. Farnham, UK: Ashgate, 2009.

[14] E. Hollnagel, *FRAM: The Functional Resonance Analysis Method - Modelling Complex Socio-technical Systems*. Aldershot, UK: Ashgate, 2012.

[15] ICAO, "Draft NOSS Manual."

[16] C. W. Johnson, B. Kirwan, and A. Licu, "The Interaction between Safety Culture and Degraded Modes: A Survey of National Infrastructures for Air Traffic Management," *Risk Manag.*, vol. 11, pp. 241–284, 2009.

[17] E. Hollnagel, *Cognitive reliability and error analysis method: CREAM*. Oxford, New York: Elsevier, 1998.

[18] G. Klein, R. Pliske, B. Crandall, and D. D. Woods, "Problem detection," *Cogn. Technol. Work*, vol. 7, pp. 14–28, 2005.

[19] L. A. Suchman, *Plans and situated actions: The problem of human machine communication*. New York: Cambridge University Press, 1987.

[20] D. D. Woods, "Essential characteristics of resilience," in *Resilience engineering: Concepts and precepts*, E. Hollnagel, D. D. Woods, and N. Leveson, Eds. Aldershot, UK: Ashgate, 2006, pp. 21–34.

[21] C. Perrow, *Normal accidents: Living with high-risk technologies*. New York, NJ: Basic Books, Inc., Publishers, 1984.

[22] E. Hollnagel, "The changing nature of risks," *Ergon. Aust.*, vol. 22, no. 1–2, pp. 33–46, 2008.

[23] DSB, "Defense Science Board Task Force Report: The Role of Autonomy in DoD Systems," Washington, DC, USA, 2012.