Reliability Engineering and System Safety 141 (2015) 115–130

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Towards understanding work-as-done in air traffic management safety assessment and design

Rogier Woltjer [a,*], Ella Pinska-Chauvin [b], Tom Laursen [c], Billy Josefsson [d]

[a] Division of Information and Aeronautical Systems, Swedish Defence Research Agency (FOI), Linköping, Sweden
[b] Directorate Air Traffic Management, Performance & Methods Unit, EUROCONTROL, Brétigny-sur-Orge, France
[c] IFATCA & Naviair, Copenhagen, Denmark
[d] Project Management and Support, NORACON/LFV Air Navigation Services of Sweden, Norrköping, Sweden

ARTICLE INFO

Available online 13 March 2015

Keywords:
Resilience engineering
Air traffic management
Work-as-done
Safety assessment
System safety
Design

ABSTRACT

This paper describes the approach taken and the results to develop guidance, to include Resilience Engineering principles in methodology 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 ATM operations. These principles are the foundation for guidance material incorporating Resilience Engineering (RE) concepts into safety assessment methodology. The guidance material provides a method using workshops generating qualitative descriptions of RE principles applied to ATM services of everyday work, as done currently and as envisioned after introduction of a new technology or way of working. The guidance material has been proposed as part of the safety assessment methodology of SESAR (Single European Sky ATM Research), and as stand-alone guidance for ATM design processes. The methodology was validated via a test case on the i4D/CTA (Controlled Time of Arrival) concept. Operational examples from the application of the developed guidance to the i4D/CTA concept are provided. Initial evaluation of the guidance suggests that the methodology (1) provides a narrative, vocabulary and documentation means of project discussions on resilience; (2) brings the discussions of safety and resilience closer to operational practice; (3) facilitates a broader systemic and integrative perspective on operational, management, business, safety, environmental, and human performance aspects; and (4) can extend the vocabulary of safety assessment to include the description of emergent properties, to better support functional changes in ATM.

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. Current EU regulation (Nr. 1035/2011) [10] requires ATM service providers to address causes and consequences of failure in safety assessment, applied to individual changes of the ATM system. The European Aviation Safety Agency [8] states that in its member states, "during the last five years (2009–2013) there were only 6 accidents that had a direct ATM contribution" (p. 63) with a total of roughly 10 million Instrument Flight Rules flights per year. Considering this very high safety record of ATM, safety management (retrospectively and prospectively) cannot be based exclusively on failure, but should attempt to understand all outcomes (positive and negative) of everyday operations [14,15]. This not only applies to the practical focus of safety management, but also to safety science: "The scientific study of safety should focus on situations where nothing goes wrong, i.e., where there is safety, rather than on situations where something goes wrong—where there is no safety" [31] (p. 24). Thus, new operational and scientific perspectives focusing on understanding everyday operations are necessary. The perspectives of Resilience Engineering [14,33,36] and Safety-II [15,30,31] aim to provide such a deepened understanding of everyday performance. In these perspectives, safety is understood as the ability to succeed under varying conditions [28].

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

* Corresponding author. Tel.: +46 13 37 85 73; fax: +46 13 37 85 50.
E-mail addresses: rogier.woltjer@foi.se (R. Woltjer), ella.pinska-chauvin@eurocontrol.int (E. Pinska-Chauvin), mettom@private.dk (T. Laursen), billy.josefsson@lfv.se (B. Josefsson).

http://dx.doi.org/10.1016/j.ress.2015.03.010
0951-8320/

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 [22,66]. The project described here aims to enhance the safety assessment process to increase the resilience (reduce the brittleness) of the future ATM system. The project does this by providing concepts and methods from Resilience Engineering to increase the SESAR program's ability to design for resilience (RE) and identify potential brittleness issues. It should however be kept in mind that also these predictions are necessarily approximate.

Adopting the RE view implies 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 [33,36].

Resilience Engineering for ATM requires an integrated and systemic approach to anticipation, monitoring, response, and learning [27,28]. Applying the Resilience Engineering perspective 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 the SESAR development phases (V1 Scope, V2 Feasibility, V3 Pre-industrial development and integration [11]) in a V-model-based development process (European Operational Concept Validation Methodology E-OCVM [11]) and the integration of Resilience Engineering guidelines for safety assessment into 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 make a step in that direction. The SESAR Safety Reference Material (SRM) (see [18]) is the process by which operational and technical projects assess safety of the concepts they develop. There is 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 the SESAR Joint Undertaking (SJU) to develop guidance for resilience to be part of the SRM, as well as transforming this safety assessment guidance into design guidelines for ATM.

Resilience Engineering is the discipline that strives to provide design and development processes, strategies, and capabilities to accomplish resilience [75]. The project reported here emphasizes the *Engineering* in Resilience Engineering and applies RE principles in a large-scale industrial setting. It focuses on how ATM resilience can be addressed in design and development. It investigates how strategies and capabilities of the ATM system to be resilient can be identified. This in turn is used to determine how changes to the ATM functional system through design and development processes change the preconditions for the ATM system to be resilient.

This article has the purpose of addressing the following research and development issue: How can the perspective of Resilience Engineering be included into the development of future systems and concepts for Air Traffic Management, through the processes of safety assessment and design in SESAR? The results of the 16.01.02 project are:

1. a SESAR working definition of resilience, a set of principles, a description of their content, and a process for addressing these principles in Safety Assessment,
2. detailed Resilience Engineering Guidance for ATM Safety Assessment, containing the definitions, principles, and the process of applying the definitions and principles, with
3. links to the SESAR processes of E-OCVM and SRM, and
4. Resilience Engineering Design Guidance for ATM.

Section 2 of this article outlines the theory that was operationalized in the project. Section 3 describes the methodology used (analyzing incidents and everyday operations) for developing resilience guidance. Section 4 describes the project results in terms of Resilience Principles and Resilience Engineering Guidance for ATM to be considered in SESAR safety assessment and design. Section 5 describes the application of the guidance to the case i4D/CTA. Sections 6 and 7 provide a short discussion and conclusion.

2. Background: Resilience engineering

Ultra-safe industrial systems [2] experience less than one accident in every 100,000 or even one million production cycles. Nuclear power generation, civil aviation, air traffic control, and various process industries may be described as ultra-safe industrial systems. Amalberti has argued that safety improvement methods that have taken the system up to this high safety level should not be further optimized but maintained, and complemented by new methods and perspectives.

These new methods and perspectives are necessary to keep up with the continuously increasing complexity of industry and society. Accident models and methods that aim to aid in explaining events and guide risk assessment need to be able to match this complexity. Resilience Engineering promotes a better understanding of what it means for systems to be resilient, how work-as-done contributes to safety and efficiency, and how trade-offs are managed. These new concepts, methods and perspectives, operationalized in this project, are defined and described in this section.

2.1. Coping with complexity

The perspectives of Resilience Engineering [33,36] and Safety-II [30,31] aim to understand and provide means to manage complexity. Complexity may be addressed in terms of coupling, interactions, and the potential for cascading effects. Coupling (loose/tight) 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 [46]. Interactions are defined as the number of variables and causal relations in the system's processes and interconnected subsystems [46]. Coupling and interactions can be related to the concept of cascading effects [66]. "The *potential for cascade* refers to how a triggering event produces a set of disturbances which can propagate and interact over lines of interdependency" [59].

2.2. Accident models and methods

Safety science has come up with a wide range of accident models since the 1930s. Accident models have been classified by Hollnagel [25] into simple linear, complex linear, and systemic accident models. Simple linear models, such as the Domino model [19] and fault/event tree models, model socio-technical systems by their physical and organizational structure and focus on linear cause-effect relationships between independent components. Complex linear models, such as the Swiss Cheese metaphor [49], also decompose socio-technical systems by their structure and consider linear relationships, but of interdependent components. Latent conditions (e.g., fatigue, bad design, management production pressure) affect how active failures (such as unsafe acts or human error) can sneak through deficiencies in