Available online at www.sciencedirect.com

SCIENCE DIRECT®

Reliability Engineering and System Safety 91 (2006) 1482–1493

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Capturing emerging complex interactions: Safety analysis in air traffic management[☆]

Massimo Felici*

LFCS, School of Informatics, The University of Edinburgh, Edinburgh EH9 3JZ, UK

Available online 15 March 2006

Abstract

The future development of air traffic management (ATM), set by the ATM 2000+ Strategy, involves a structural revision of ATM processes, a new ATM concept and a system approach for the ATM network. This requires ATM services to go through significant structural, operational and cultural changes that will contribute towards the ATM 2000+ Strategy. Moreover, from a technology viewpoint, future ATM services will employ new systems forming the emergent ATM architecture underlying and supporting the European Commission's Single European Sky Initiative. Introducing safety relevant systems in ATM contexts requires us to understand the risk involved in order to mitigate the impact of possible failures. This paper is concerned with some limitations of safety analysis with respect to operational aspects of introducing new systems (functionalities).

Keywords: Safety analysis; Air traffic management; Complex interactions; System evolution

1. Introduction

The future development of air traffic management (ATM), set by the ATM 2000+ Strategy [1], involves a structural revision of ATM processes, a new ATM concept and a system approach for the ATM network. The overall objective [1] is, *for all phases of flight, to enable the safe, economic, expeditious and orderly flow of traffic through the provision of ATM services, which are adaptable and scalable to the requirements of all users and areas of European airspace*. This requires ATM services to go through significant structural, operational and cultural changes that will contribute towards the ATM 2000+ Strategy. Moreover, from a technology viewpoint, future ATM services will employ new systems forming the emergent ATM architecture underlying and supporting the European Commission's Single European Sky Initiative.

ATM services, it is foreseen, will need to accommodate an increasing traffic, as many as twice number of flights, by 2020. This challenging target will require cost-effective gaining of extra capacity together with the increase of safety levels [2,3]. Enhancing safety levels affects the ability to accommodate increased traffic demand as well as the operational efficiency of ensuring safe separation between aircrafts. Suitable safe conditions shall precede the achievement of increased capacity (in terms of accommodated flights). Therefore, it is necessary to foresee and mitigate safety issues in aviation where ATM can potentiality deliver safety improvements.

Introducing safety relevant systems in ATM contexts requires us to understand the risk involved in order to mitigate the impact of possible failures. Safety analysis involves the activities, i.e., definition and identification of system(s) under analysis, risk analysis in terms of tolerable severity and frequency, definition of mitigation actions, that allow the systematic identification of hazards, risk assessment and mitigation processes in critical systems [4,5]. This paper is concerned with some limitations of safety analysis with respect to operational aspects of introducing a new system (functionality). In particular, emerging complex interactions affect the overall system

[☆] This work has been supported by the UK EPSRC Interdisciplinary Research Collaboration in Dependability, DIRC—http://www.dirc.org.uk—Grant GR/N13999.

*Tel.: +44 131 650 5899.

E-mail address: mfelici@inf.ed.ac.uk.

URL: http://homepages.inf.ed.ac.uk/mfelici/.

0951-8320/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2006.01.010

safety. In order to capture these interactions, it is necessary to adopt an evolutionary approach to safety analysis [6]. This paper introduces an evolutionary framework, which supports evolutionary safety analysis. The paper is structured as follows. Section 2 introduces safety analysis in ATM domain. The EUROCONTROL Safety Regulatory Requirement [7], ESARR4, requires the use of a risk based-approach in ATM when introducing and/or planning changes to any (ground as well as onboard) part of the ATM system. Unfortunately, ATM systems, procedures and interactions expose limitations of safety analysis. Section 3 shows an example of complex interactions drawn from the ATM domain. The accident (1st July 2002) between a Boeing B757-200 and a Tupolev TU154M [8], that caused the fatal injuries of 71 persons, provides an instance of unforeseen complex interactions. These interactions triggered a catastrophic failure, although all aircraft systems were functioning properly. Section 4 proposes a framework for capturing complex interactions. The framework supports evolutionary safety analysis [6]. Section 5, finally, discusses the proposed framework and draws some conclusions.

2. Safety analysis in ATM

ATM services across Europe are constantly changing in order to fulfil the requirements identified by the ATM 2000+ Strategy [1]. Currently, ATM services are going through a structural revision of processes, systems and underlying ATM concepts. This highlights a system approach for the ATM network. The delivery and deployment of new systems will let a new ATM architecture to emerge. The EUROCONTROL OATA project [9] intends to deliver the concepts of operation, the logical architecture in the form of a description of the interoperable system modules, and the Architecture Evolution Plan. All this will form the basis for common European regulations as part of the Single European Sky.

The increasing integration, automation and complexity of the ATM system requires a systematic and structured approach to risk assessment and mitigation, including hazard identification, as well as the use of predictive and monitoring techniques to assist in these processes. Faults [10] in the design, operation or maintenance of the ATM system or errors in the ATM system could affect the safety margins (e.g., loss of separation) and result in, or contribute to, an increased hazard to aircrafts or a failure (e.g., a loss of separation and an accident in the worst case). Increasingly, the ATM system relies on the reliance (e.g., the ability to recover from failures and accommodate errors) and safety (e.g., the ability to guarantee failure independence) features placed upon all system parts. Moreover, the increased interaction of ATM across state boundaries requires that a consistent and more structured approach be taken to the risk assessment and mitigation of all ATM system elements throughout the ECAC (European Civil Aviation Conference) states [11]. Although the average trends show a decrease in the number of fatal accidents for Europe, the approach and landing accidents are still the most safety pressing problems facing the aviation industry [12–14]. Many relevant repositories[1] report critical incidents involving the ATM system. Unfortunately, even maintaining the same safety levels across the European airspace would be insufficient to accommodate an increasing traffic without affecting the overall safety of the ATM system [15].

Diverse domains (e.g., nuclear, chemical or transportation) adopt safety analysis that originate from a general approach [4,5]. Recent safety requirements, defined by EUROCONTROL (European organization for the safety of air navigation), imply the adoption of a similar safety analysis for the introduction of new systems and their related procedures in the ATM domain [7]. Unfortunately, ATM systems and procedures have distinct characteristics[2] (e.g., openness, volatility, etc.) that expose limitations of the approach. In particular, the complete identification of the system under analysis is crucial for its influence on the cost and the effectiveness of the safety analysis. Some safety-critical domains (e.g., nuclear and chemical plants) allow proper application of conventional safety analyses. Physical design structures constrain system's interactions and stress the separation of safety related components from other system parts. This ensures the independence of failures. In contrast, ATM systems operate in open and dynamic environments where it is difficult completely to identify system interactions. For instance, there exist complex interactions between aircraft systems and ATM safety relevant systems. Unfortunately, these complex interactions may give rise to catastrophic failures. Hence, safety analysis has to take into account these complex interaction mechanisms (e.g., failure dependence, reliance in ATM, etc.) in order to guarantee and even increase the overall ATM safety as envisaged by the ATM 2000+ Strategy.

The introduction of new safety relevant systems in ATM contexts requires us to understand the risk involved in order to mitigate the impact of possible failures. The EUROCONTROL Safety Regulatory Requirement [7],

[1] Some repositories are: Aviation Safety Reporting Systems—http://asrs.arc.nasa.gov/; Aviation Safety Network—http://aviation-safety.net/; Flight Safety Foundation: An International Organization for Everyone Concerned With Safety of Flight—http://www.flightsafety.org/; Computer-Related Incidents with Commercial Aircraft: A Compendium of Resources, Reports, Research, Discussion and Commentary compiled by Peter B. Ladkin et al.—http://www.rvs.uni-bielefeld.de/publications/Incidents/.

[2] There are some unique structural conditions in this industry that promote safety, and despite complexity and coupling, technological fixes can work in some areas. Yet we continue to have accidents because aircraft and the airways still remain somewhat complex and tightly coupled, but also because those in charge continue to push the system to its limits. Fortunately, the technology and the skilled pilots and air traffic controllers remain a bit ahead of the pressures, and the result has been that safety has continued to increase, though not as markedly as in early decades [16, p. 123].

ESARR4, requires the use of a risk based-approach in ATM when introducing and/or planning changes to any (ground as well as onboard) part of the ATM system. This concerns the human, procedural and equipment (i.e., hardware or software) elements of the ATM system as well as its environment of operations at any stage of the life cycle of the ATM system. The ESARR4 [7] requires that ATM service providers systematically identify any hazard for any change into the ATM system (parts). Moreover, they have to assess any related risk and identify relevant mitigation actions. In order to provide guidelines for and standardise safety analysis EUROCONTROL has developed the EATMP safety assessment methodology (SAM) [17] reflecting best practices for safety assessment of air navigation systems.

2.1. The safety assessment methodology

The SAM provides a means of compliance to ESARR4. The objective of the methodology is to define the means for providing assurance that an air navigation system is safe for operational use. The SAM methodology describes a generic process for the safety assessment of air navigation systems. This process consists of three major steps: *functional hazard assessment* (*FHA*), *preliminary system safety assessment* (*PSSA*) and *system safety assessment* (*SSA*). Fig. 1 shows how the SAM methodology contributes towards system assurance. The process covers the complete life cycle of an air navigation system, from initial system definition, through design, implementation, integration, transfer to operations, to operations and maintenance. Moreover, it takes into account three different types of system elements (human, procedure and equipment elements), the interactions between these elements and the interactions between the system and its environment.

The FHA is a top-down iterative process, initiated at the beginning of the development or modification of an air navigation system. The objective of the FHA process is to determine the overall safety requirements of the system (i.e., specifies the safety level to be achieved by the system). The process points out potential functional failure modes and hazards. It assesses the consequences of their occurrences on the safety of operations, including aircraft operations, within a specified operational environment. The FHA process specifies overall safety objectives of the system. The PSSA is another top-down iterative process, initiated at the beginning of a new design or modification to an existing design of an air navigation system. The objective of performing a PSSA is to demonstrate whether the assessed system architecture can reasonably be expected to achieve the safety objectives specified in the FHA. The PSSA process the safety objectives into safety requirements allocated to the system elements. That is, it identifies the risk level to be achieved by each system element. The SSA is a process initiated at the beginning of the implementation of an air navigation system. The objective of performing a SSA is to demonstrate that the implemented system achieves an acceptable (or at least tolerable) risk and consequently satisfies its safety objectives specified in the FHA. Moreover, the SSA assesses whether each system element meets its safety requirements specified in the PSSA. The SSA process collects evidences and provides assurance throughout the system life cycle (i.e., from implementation to decommissioning).

Although the SAM methodology describes the underlying principles of the safety assessment process, it provides limited information to applying these principles in specific contexts.[3] The hazard identification, risk assessment and mitigation processes comprise a determination of the scope, boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate. This supports the identification and validation of safety requirements on the constituent parts.

2.2. Limitations

Conventional safety analyses are deemed acceptable in domains such as the nuclear or the chemical sector. Nuclear or chemical plants are well-confined entities with limited predictable interactions with the surroundings. In nuclear and chemical plants design stresses the separation of safety related components from other plant systems. This ensures the independence of failures. Therefore, in these application domains it is possible to identify acceptable tradeoffs between completeness and manageability during the definition and identification of the system under analysis. In contrast, ATM systems operate in open and dynamic environments. Hence, it is difficult to identify the full picture of system interactions in ATM contexts. In particular:

- There is a complex interaction between aircrafts' controls and ATM safety functions. Unfortunately, this complex interaction may give rise to catastrophic failures. Hence, failure separation (i.e., understanding the mechanisms to enhance failure independence) would increase the overall ATM safety.
- Humans [19,20] using complex language and procedures mediate this interaction. Moreover, most of the final decisions are still demanded to humans whose behaviour is less predictable than that of automated systems. It is necessary further to understand how humans use external artefacts (e.g., tools) to mediate this interaction.

[3] Additional Recommendation 9: [...] Appropriate procedures and principles were in place within Swiss Air Traffic Management and it seems clear that had these been followed then the controllers might not have been exposed to such demanding operating conditions. It follows that EUROCONTOL and the ICAO might, therefore, usefully provide additional services in helping organisations implement these good practices and where appropriate might assist national regulators in monitoring their implementation [18, p. 45].

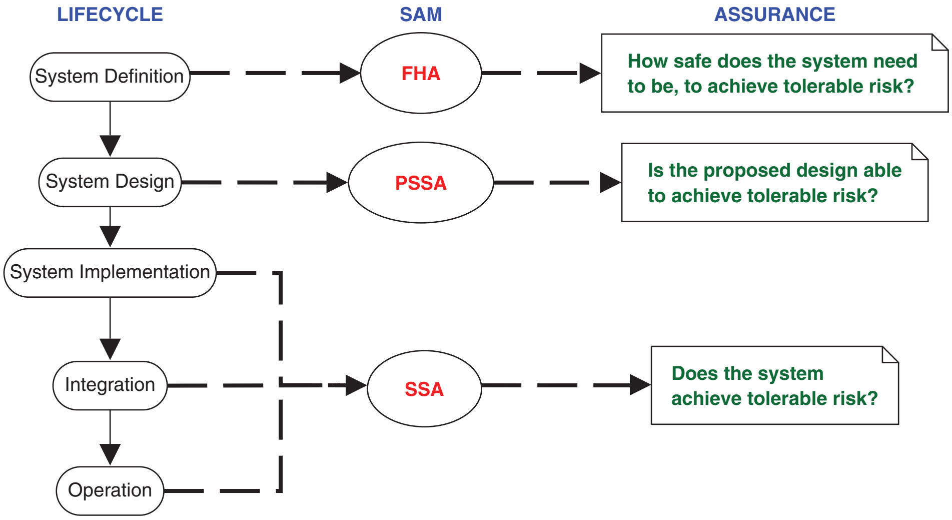
LIFECYCLE
SAM
ASSURANCE
System Definition
FHA
How safe does the system need to be, to achieve tolerable risk?
System Design
PSSA
Is the proposed design able to achieve tolerable risk?
System Implementation
Integration
SSA
Does the system achieve tolerable risk?
Operation

Fig. 1. Contribution of the safety assessment methodology towards system assurance with respect to the lifecycle.

Moreover, this will allow the understanding of how humans adopt technological artefacts and adapt their behaviours in order to accommodate ATM technological evolution. Unfortunately, the evolution of technological systems often corresponds to a decrease in technology trust affecting work practice.

- Work practice and systems evolve rapidly in response to demand and a culture of continuous improvements. A comprehensive account of ATM systems, moreover, will allow the modelling of the mechanisms of evolution. This will enhance strategies for deploying new system configurations or major system upgrades. On the one hand modelling and understanding system evolution support the engineering of (evolving) ATM systems. On the other hand modelling and understanding system evolution allow the communication of changes across different organisational levels. This would enhance visibility of system evolution as well as trust in transition to operations.

3. Complex interactions

This section shows an example of complex interactions drawn from the ATM domain. The ATM domain highlights how safety-critical activities rely on complex socio-technical interactions. *Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible* [16]. Interactions are means for enabling the (re)distribution of knowledge among heterogeneous actors and resources. The distribution of knowledge and its interaction strategies allow the characterisation of socio-technical interactions [21]. These complex interactions expose the limitations of safety analysis.

On 1st July 2002 two airplanes, a Tupolev TU 154 M on its flight from Moscow (Russia) to Barcelona (Spain), and a Boeing B757 on its flight from Bergamo (Italy) to Brussels (Belgium), collided while on flight. The collision caused the catastrophic destruction of both airplanes and the loss of all passengers [8]. A systemic analysis of the accident provides a convenient viewpoint in order to highlight complex interactions. The analysis shows that interactions in socio-technical systems redistribute critical knowledge to carrying out technology-mediated activities [22]. Although human factors are often over emphasised as a principal cause in aviation accidents [23], system failures are often strongly related to organisational failures [23–25]. The reconstruction of the accident points out heterogeneous aspects and multiple causes [8,18,26].

The systemic reconstruction of the accident uses a representation that highlights the interactions among heterogeneous resources. The resource model [21] identifies a limited number of resource types as abstract information structures that can be used to analyse interactions. The resource model [21] defines the concept of interaction strategy to describe the way in which different configurations of resources can differently shape human activities. These elements of the resource model (i.e., information structures and interaction strategies) find grounds in *distributed cognition*. Distributed cognition [27] focuses on the interaction between representational resources, which can be located within human mind as well as external artefacts. It helps to understand how information mediated activities [28–30] are carried out by distributed resources.[4] Distributed cognition stresses that human cognition is unbounded within human minds, but it extends to external distributed artefacts. Socio-technical systems consist of internal and external artefacts interacting each other. A holistic representation of socio-technical systems highlights interactions among heterogeneous resources. For instance, the SHEL model [31] defines any (electronic mediated)

[4] Additional Recommendation 8: Further thought should be given to the verbal protocols governing the exchange of information between controllers and the crews of all aircraft involved in a TCAS incident. [...] [18, p. 21].

productive process as performed by a combination of Hardware (e.g., any material tool used in the process execution), Software (e.g., procedures, rules, practices, etc.) and Liveware (e.g., end-users, managers, etc.) resources embedded in a given Environment (e.g., socio-cultural, political, etc.). Hence any productive process may be regarded as an instantiation of the SHEL model for a specific process execution. As the SHEL model emphasises that any productive process relies on the different resources, distributed cognition and resources-based modelling (e.g., like the SHEL model) show different aspects of socio-technical systems that may be linked together in a sound way [21]. Simple models representing human understandings with respect to socio-technical systems have stimulated the use of mechanised verification methods in order to identify automation surprises [32]. The results encourage further investigations on the use of mechanised tools in order to identify inconsistencies in the design of socio-technical systems. Note that the above features may be identified in other contexts as well (e.g., healthcare [33]). Nowadays technology is pervasive. Human activities depend on technical systems. The basics on which socio-technical systems rely on can thus be generalised.

Table 1 shows a SHEL description of the case study. The accident [8,18] involved the following main resources, i.e., Liveware (L), Hardware (H), and Software (S) embedded in an Environment (E): Air Traffic Controller (ATCer), Crew of the Boeing B757 ($\mathtt{C_B}$), Crew of the Tupolev TU 154 ($\mathtt{C_T}$) and the two TCAS systems (respectively, $\mathtt{TCAS_B}$ and $\mathtt{TCAS_T}$). At the moment of the collision one controller (ATCer) was on the sector controller workplace. The controller had to monitor two workplaces with radar screens. The controller followed training programs for TCAS. There were other controllers, but they were inactive in the considered scenario. Both aircraft crews (i.e., $\mathtt{C_B}$ and $\mathtt{C_T}$) completed the corresponding training for TCAS. Both aircrafts were equipped with identical collision avoidance systems, TCAS [34] (i.e., $\mathtt{TCAS_B}$ and $\mathtt{TCAS_T}$). Neither the history of the flight nor the evaluation of the flight data recorders indicated any technical defects on the aircrafts. The operational aspects involve the relevant procedures that apply in the specific case, e.g., procedures in case of TCAS resolution. In the Swiss Air Traffic Control maintenance work of the system was performed in the late evening of the accident day. During this period of time the ground based collision warning system STCA (Short term conflict alert) was providing limited functionalities. The direct phone connections to the adjacent air traffic control services were unavailable either. Other technology was available in the environment, but it was irrelevant in the accident.

Table 1
A SHEL description of the case study

Resource	Type	Description
ATCer	L	Air traffic controller
$\mathtt{C_T}$	L	Aircraft crews
$\mathtt{C_B}$	L	
$\mathtt{TCAS_T}$	H S	TCAS systems
$\mathtt{TCAS_B}$	H S	
Operating procedures	S	Operating procedures
Environment	E	Operating environment

Table 2 shows the chain of events that caused the accident. Initially, at time t_1, both aircraft crews get a traffic advisory by the TCAS systems, respectively. Then, the complex interactions between the diverse system resources affect the overall safety. Although both aircrafts were equipped with similar TCAS systems, human mediation and response give rise to unsafe conditions causing the collision at time t_8. The knowledge distribution among (or knowledge gap between) Liveware resources (i.e., air traffic controller and aircraft crews) is highly critical [22]. For instance, air traffic controllers may often have poor information on aircraft capabilities, weather and winds that are needed for making their own assessment of whether an aircraft will be able to conform to a clearance as expected. Air traffic controllers are unaware of what the TCAS system on an aircraft is advising the aircraft crew to do. The scenario reconstruction in Table 2 shows that the ATCer knows that $\mathtt{C_B}$ is following a resolution advisory (RA) at time t_6, when $\mathtt{C_B}$ reports it to the ATCer. The scenario reconstruction reports only the main interactions. Note that the granularity and the focus of the information affect the accident analysis [18].

The simple systemic reconstruction of the accident scenario points out two of the critical factors in the accident: *timeliness* and *knowledge*. ATM scenarios consist of timed sequences of events involving hybrid interactions (e.g., human–machine interaction, human–human interaction). The timing aspects of these interactions affect operational aspects (e.g., procedures) as well as the whole system safety.[5] The sequence of events consists of interactions that continuously modify the distribution of knowledge. The accident sequence of events seems similar to many other sequences, it "just" differs in the final collision. It seems that the sequence of events lacks of early risk perception. However, additional recommendations[6] highlight how early warnings could have been identified, if risk assessment would have been conducted on early accidents. This stresses the need for pro-active and iterative approaches to risk analysis, hence safety analysis [6].

[5] Safety Recommendation No. 12/2004: [...] the radar system of the air traffic control service provider is technically equipped in a way that enables display updates within 8 s or less in en route airspace [8, p. 113].

[6] Additional Recommendation 10: The [...] accident was pre-dated by two [...] accidents [...] that eloquently illustrated the danger of Single Man Operating Procedures even under more benign circumstances that existed on the night of the accident. EUROCONTROL ESSAR guidelines require that such incidents should normally trigger a formal risk assessment and yet this was not done in either of these cases [...] [18, p. 45].

Table 2
Accident scenario

Time	Actors	Event(s)
t_1	$\texttt{TCAS}_\texttt{B}$, $\texttt{C}_\texttt{B}$ $\texttt{TCAS}_\texttt{T}$, $\texttt{C}_\texttt{T}$	The TCAS on both aircrafts give a Traffic Advisory
t_2	$\texttt{ATCer}$, $\texttt{C}_\texttt{T}$	ATCer tells CT: "descend flight level 350, expedite, I have crossing traffic"
t_3	$\texttt{TCAS}_\texttt{B}$, $\texttt{C}_\texttt{B}$ $\texttt{TCAS}_\texttt{T}$, $\texttt{C}_\texttt{T}$	Both aircrafts get a TCAS Resolution Advisory (RA); CB complies; CT remains at FL360
t_4	$\texttt{ATCer}$, $\texttt{C}_\texttt{T}$	ATCer repeats the instruction to CT to descend; CT complies
t_5	$\texttt{TCAS}_\texttt{B}$, $\texttt{C}_\texttt{B}$	"Increase descent"
t_6	$\texttt{C}_\texttt{B}$, $\texttt{ATCer}$	CB report to ATCer that they are doing a TCAS descend
t_7	$\texttt{TCAS}_\texttt{T}$, $\texttt{C}_\texttt{T}$	"Increase climb"
t_8		Collision

The analysis with respect to the TCAS system points out how the prompt pilot's response is necessary in order to maintain safety.[7] The safety benefits provided by TCAS are directly dependent on a pilot's response to a RA. The pilots' instinctive reaction to a RA should always be to respond to the RA in the direction and the degree displayed. Knowledge continuously evolves as a consequence of the occurrences of human actions and interactions. Both pilots and the controller had partial knowledge about the real situation. Each one acquired different knowledge and understanding about the situation. Hence, each one differently perceived the criticality of the situation. This highlights cognitive aspects play an important role in risk perception in critical situations.[8] Pro-active and iterative risk analysis, safety analysis, would allow to take into account the subtle operational aspects that characterise complex interactions. Perceived risk is therefore an outcome between organisational aspects (e.g., social structures) [35], system dependability and system usage [24]. Future ATM illustrates *risk homeostasis*[9] in practice [24]. The expected traffic growth would, of course, require to improve the capacity (by reducing separation between airplanes) and to increase the number of monitored aircrafts per controller. In order to maintain the same risk perception, the efficiency and dependability of the system must be increased [15,36]. This involves a structural revision of ATM processes, a new ATM concept and a systems approach for the ATM network. This requires ATM services to go through significant structural, operational and cultural changes that will contribute towards the ATM 2000+ Strategy.

4. Evolutionary safety analysis

Capturing cycles of discoveries and exploitations during system design involves the identification of mappings between socio-technical solutions and problems. The proposed framework exploits these mappings in order to construct an evolutionary model that enhances safety analysis. Fig. 2 shows the proposed framework, which captures these evolutionary cycles at different levels of abstraction and on diverse models. The framework consists of three different hierarchical layers: *system modelling transformation* (*SMT*), *safety analysis modelling transformation* (*SAMT*) and *operational modelling transformation* (*OMT*). The remainder of this section describes the three hierarchical layers.

4.1. System modelling transformation

The definition and identification of the system under analysis is extremely critical in the ATM domain. System models used during the design phase provide limited support to safety as well as risk analysis. This is because existing models defined in the design phase are adapted and reused for safety and risk analysis. Organisational and cost-related reasons often determine this choice, without questioning whether models are suitable for the intended use. The main drawback is that design models are tailored to support the work of system designers. Thus, system models capture characteristics that may be of primary importance for design, but irrelevant for safety analysis. Models should be working-tools that, depending on their intended use, ease and support specific activities and cognitive operations of users.

Modelling methodologies and languages advocate different design strategies. Although these strategies support different aspects of software development, they originate in a common *systems approach*[10] to solving complex problems

[7] Safety Recommendation No. 18/2002: [...] pilots flying are required to obey and follow TCAS resolution advisories (RAs), regardless of whether contrary ATC instruction is given prior to, during, or after the RAs are issued. Unless the situation is too dangerous to comply, the pilot flying should comply with the RA until TCAS indicates the airplane is clear of the conflict [8, p. 111].

[8] Additional Recommendation 7: A subsequent analysis of the accident should be conducted to identify the cognitive and perceptual cues that helped the controller to identify the potential conflict. [...] [18, p. 21].

[9] Risk homeostasis: [...] advances in technology lead to a reduction in perceived risk, hence to behaviour that is closer to the limits of acceptable performance—thereby effectively reducing the margin for safety. It is quite a paradox that the technological improvements do not seem to lead to a reduction in the overall number of malfunctions, but rather to an increase in their severity [24, pp. 3–4].

[10] Practitioners and proponents embrace a holistic vision. They focus on the interconnections among subsystems and components, taking special note of the interfaces among various parts. What is significant is that system builders include heterogeneous components, such as mechanical, electrical, and organizational parts, in a single system. Organizational parts might be managerial structures, such as a military command, or political entities, such as a government bureau. Organizational components not only interact with technical ones but often reflect their

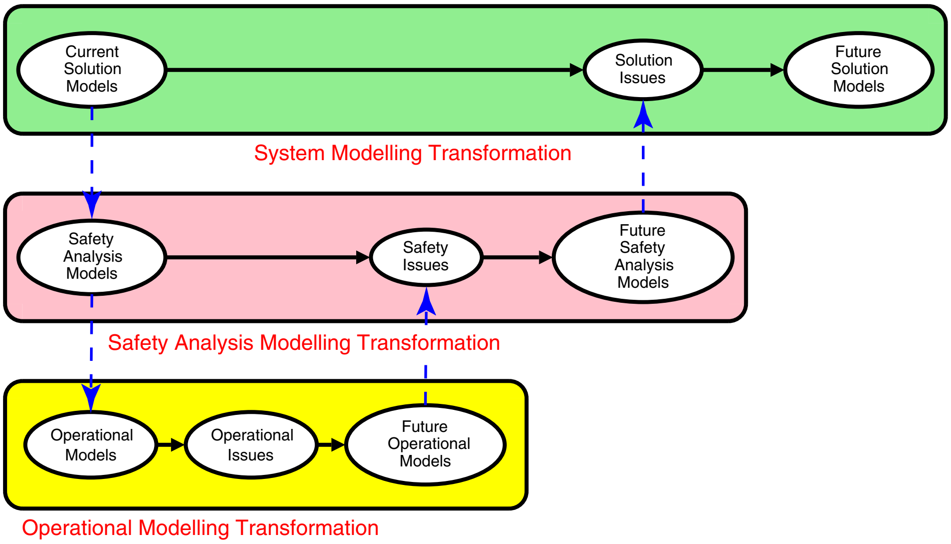
Current Solution Models
Solution Issues
Future Solution Models
System Modelling Transformation
Safety Analysis Models
Safety Issues
Future Safety Analysis Models
Safety Analysis Modelling Transformation
Operational Models
Operational Issues
Future Operational Models
Operational Modelling Transformation

Fig. 2. A framework for modelling evolutionary safety analyses.

and managing complex systems. Modelling incorporates design concepts and formalities into system specifications. This enhances our ability to assess safety requirements. For instance, *software cost reduction* (SCR) consists of a set of techniques for designing software systems [38,39]. In order to minimise the impact of changes, separate system modules have to implement those system features that are likely to change. Although module decomposition reduces the cost of system development and maintenance, it provides limited support for system evolution. *Intent specifications* provide another example of modelling that further supports the analysis and design of evolving systems [40]. In accordance with the notion of semantic coupling, intent specifications support strategies (e.g., eliminating tightly coupled mappings) to reduce the cascade effect of changes. Although these strategies support the analysis and design of evolving systems, they provide limited support to understand the evolution of high-level system requirements.[11]

Heterogeneous engineering[12] provides a different perspective that further explains the complex interaction between system (specification) and environment. Heterogeneous engineering provides a convenient comprehensive viewpoint for the analysis of the evolution of socio-technical systems. Heterogeneous engineering involves both the systems approach [37] as well as the social shaping of technology [42]. According to heterogeneous engineering, system requirements specify mappings between problem and solution spaces [43,44]. Both spaces are socially constructed and negotiated through sequences of mappings between solution spaces and problem spaces [43,44]. Therefore, system requirements emerge as a set of consecutive solution spaces justified by a problem space of concerns to stakeholders. Requirements, as mappings between socio-technical solutions and problems, represent an account of the history of socio-technical issues arising and being solved within industrial settings [43–45]. The formal extension of these mappings (or solution space transformations) identifies a framework to model and capture evolutionary system features (e.g., requirements evolution, evolutionary dependencies, etc.) [45].

SMT captures how solution models evolve in order to accommodate design issues or evolving requirements. Therefore, an SMT captures system requirements as mappings between socio-technical solutions and problems. This allows the gathering of changes into design solutions. That is, it is possible to identify how changes affect design solution. Moreover, this enables sensitivity analyses of design changes. In particular, this allows the revision of safety requirements and the identification of hazards due to the introduction of a new system. Therefore, the SMT supports the gathering of safety requirements for evolving systems. That is, it supports the main activities occurring during the top-down iterative process FHA in the SAM

(*footnote continued*)
characteristics. For instance, a management organization for presiding over the development of an intercontinental missile system might be divided into divisions that mirror the parts of the missile being designed [37, Introduction, p. 3].

[11] Leveson in [40] reports the problem caused by Reversals in TCAS (traffic alert and collision avoidance system): About four years later the original TCAS specification was written, experts discovered that it did not adequately cover requirements involving the case where the pilot of an intruder aircraft does not follow his or her TCAS advisory and thus TCAS must change the advisory to its own pilot. This change in basic requirements caused extensive changes in the TCAS design, some of which introduced additional subtle problems and errors that took years to discover and rectify.

[12] People had to be engineered, too—persuaded to suspend their doubts, induced to provide resources, trained and motivated to play their parts in a production process unprecedented in its demands. Successfully inventing the technology, turned out to be heterogeneous engineering, the engineering of the social as well as the physical world [41, p. 28].

methodology [17]. The FHA in the SAM methodology then initiates another top-down iterative approach, i.e., the PSSA. Similarly, the framework considers design solutions and safety objectives as input to safety analysis. Safety analysis assesses whether the proposed design solution satisfies the identified safety objectives. This phase involves different methodologies (e.g., fault tree analysis, HAZOP, etc.) that produce diverse (system) models. System usage or operational trials may give rise to unforeseen safety issues that invalidate (part of) safety models. In order to take into account these issues, it is necessary to modify safety analysis. Therefore, safety analysis models evolve too.

4.2. Safety analysis modelling transformation

The failure of safety-critical systems highlights safety issues [4,5,16,46]. It is often the case that diverse causes interacted and triggered particular unsafe conditions. Although safety analysis (i.e., safety case) argues system safety, complex interactions, giving rise to failures, expose the limits of safety arguments. Therefore, it is necessary to take into account changes in safety arguments [47]. Fig. 3 shows an enhanced safety-case lifecycle [47].

The lifecycle identifies a general process for the revision of safety cases. Greenwell et al. in [47] motivate the safety-case lifecycle by evolutionary (safety-case) examples drawn from the aviation domain. Figs. 4 and 5 show subsequent versions of a safety case. The graphical notation that represents the safety cases is the goal structuring notation (GSN) [48]. Although GSN addresses the maintenance of safety cases, the approach provides limited support with respect to complex dependencies (e.g., external to the safety argument) [49,50]. Moreover, it lacks any interpretation of the relationships between subsequent safety cases.

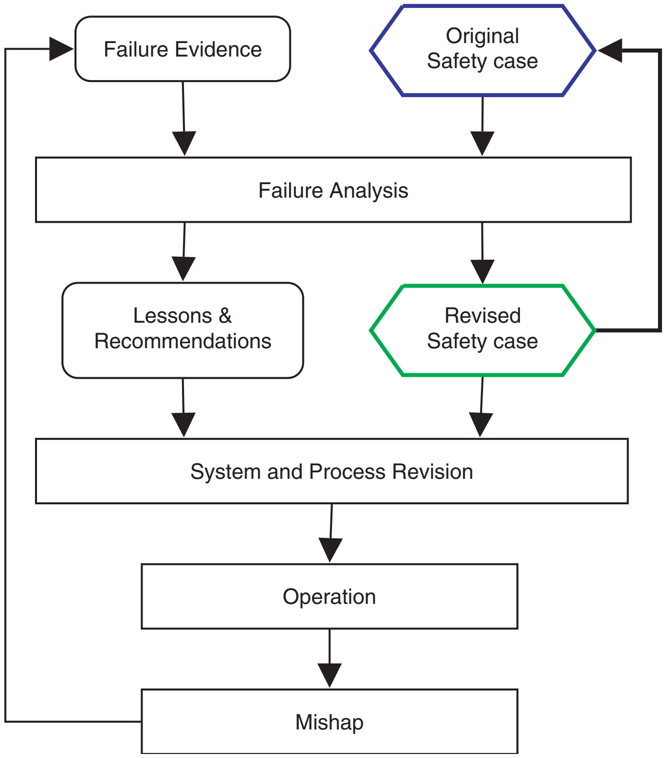

Fig. 3. The enhanced safety-case lifecycle [47].

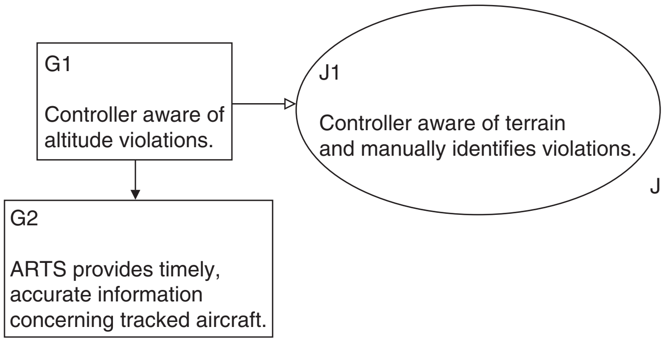
G1
Controller aware of altitude violations.
J1
Controller aware of terrain and manually identifies violations.
J
G2
ARTS provides timely, accurate information concerning tracked aircraft.

Fig. 4. Initial safety argument.

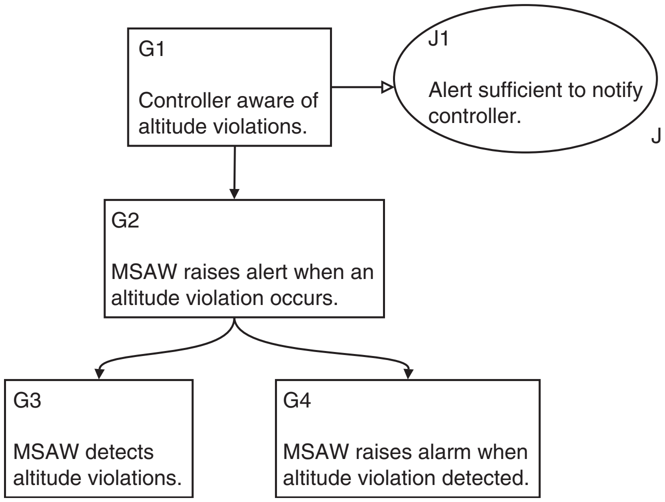
G1
Controller aware of altitude violations.
J1
Alert sufficient to notify controller.
J
G2
MSAW raises alert when an altitude violation occurs.
G3
MSAW detects altitude violations.
G4
MSAW raises alarm when altitude violation detected.

Fig. 5. Revised safety argument.

Fig. 4 shows the initial safety case arguing: "*Controller aware of altitude violations*". Unfortunately, an accident invalidates the justification J1. The satisfaction of the subgoal G2 is insufficient for the satisfaction of the goal G1. Fig. 5 shows the revised safety case that addresses the issue occurred. Unfortunately, another accident, again, invalidates the second safety case [47]. Hence, the safety argument needs further revision in order to address the safety flaw uncovered by the accident.

Fig. 6 shows a safety space transformation that captures the safety case changes [45]. The safety case transformation captures the changes from the initial safety case $\mathscr{M}_i^t$ (see, Fig. 4) to the revised safety case $\mathscr{M}_i^{t+1}$ (see, Fig. 5). An accident invalidates the justification J1. The satisfaction of the subgoal G2 is insufficient for the satisfaction of the goal G1. The proposed safety problem space, $\mathscr{P}_t$, contains these problems, i.e., P_j^t and P_{j+1}^t. The safety space transformation addresses the highlighted problems into the proposed safety case $\mathscr{M}_i^{t+1}$. In order to address the highlighted problems, it is necessary to change the initial safety case.

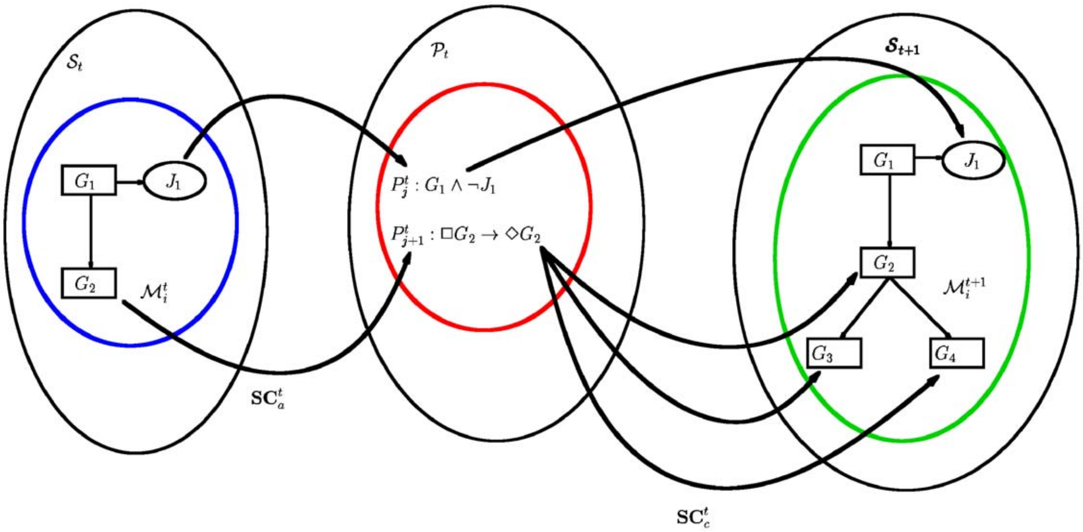

Fig. 6. A safety space transformation.

The proposed changes are taken into account in the proposed safety case. Note that there might be different proposed safety cases addressing the proposed safety problem space. The safety space transformation identifies the safety case construction and judgement in terms of safety argumentations and constraints. The safety case consists of the collections of mappings between safety cases and problems. The first part of a safety case consists of the safety argumentations, which capture the relationship that comes from safety cases looking for problems. The second part of a safety case consists of the safety constraints, which capture how future safety cases address given problems. Safety cases at any given time, *t*, can be represented as the set of all the arcs, that reflect the contextualised connections between the problem space and the current and future safety space. The definition of safety case transformation enables us further to interpret and understand safety case changes, hence safety case evolution [45].

SAMT captures how safety analysis models evolve in order to accommodate emerging safety issues. Note that the formal framework is similar to the one that captures SMT. Although design models serve as a basis for safety models, they provide limited supports to capture unforeseen system interactions. Therefore, SAMT supports those activities involved in the PSSA process of the SAM methodology [17]. Note that although the SAM methodology stresses that both FHA and PSSA are iterative processes, it provides little supports to manage processess iterations as well as system evolution in terms of design solution and safety requirements. The framework supports these evolutionary processes.

Table 3
The main problem areas occurring in two sample incident reports

Problem areas	Controller reports	TCAS II incidents
ATC facility	2	
ATC human performance	44	39
Flight crew human performance	26	40
Cabin crew human performance	1	
Aircraft	3	10
Weather	4	3
Environmental factor	8	6
Airspace structure	5	18
Navigational facility	6	4
Airport	5	5
FAA	3	5
Chart or publication	1	
Maintenance human performance	1	
Company		1

4.3. Operational modelling transformation

Operational models (e.g., structured scenarios, patterns of interactions, structured procedures, workflows, etc.) capture heterogeneous system dynamics. Unfortunately, operational profiles often change with system usage (in order to integrate different functionalities or to accommodate system failures). Table 3 shows the main problems areas identified in reported incidents: Controller Reports [51] and TCAS II Incidents [52]. Both reports consist of the 50 most recent relevant aviation safety reporting system (ASRS) reports. The small samples are insufficient to identify prevalent issues. However, the two reports highlight the complexity and the coupling within the ATM domain [16]. In particular, the most critical problem areas are the performance of air traffic controllers and aircraft crews in both sets of reports. This highlights the coupling between ground and onboard systems, hence the complex interactions in ATM. The analysis of the reports is in agreement with other studies [53,54] that analyse human errors as organisational failures [4,24,25].

Technically, operational observations are reported anomalies (or faults), which may trigger errors eventually resulting in failures. These observations capture *erroneous actions* [24]: "An erroneous action can be defined as an action which fails to produce the expected result and/or which produces an unwanted consequence". In the context of heterogeneous systems (or man–machine systems, or socio-technical systems), erroneous actions usually occur in the interfaces or interactions (e.g., man–machine interactions). The cause of erroneous actions can logically lie with either human beings, systems and/or conditions when actions were carried out. Erroneous actions can occur on all system levels and at any stage of the lifecycle.

Capturing operational interactions and procedures allows the analysis of human reliability [24]. In a continuously changing environment like ATM, adaption enhances the coupling between man and machine [55]. Hollnagel in [55] identifies three different adaption strategies: *adaption through design*, *adaption through performance* and *adaption through management*. OMT captures how operational models change in order to accommodate issues arising. The evolution of operation models informs safety analyses of new hazards. Therefore, OMT supports the activities involved in the SSA process of the SAM methodology.

5. Discussion and conclusions

In order to realistically and cost-effectively realise the ATM 2000+ Strategy, systems from different suppliers will be interconnected to form a complete functional and operational environment, covering ground segments and aerospace. Industry will be involved as early as possible in the lifecycle of ATM projects. EUROCONTROL manages the processes that involve the definition and validation of new ATM solutions using industry capabilities (e.g., SMEs). SMEs are often involved at different stages of the lifecycle of ATM projects. In particular, SMEs, as part of the validation process, conduct safety analyses, although they may indirectly be involved in the design and development of ATM-related systems. Specialised SMEs provide specific competencies and safety expertise required for this critical activity. SMEs face the problem of the definition and identification of the system under analysis and its interactions. In practice, safety analyses adapt and reuse system design models (produced by third parties). Technical, organisational and cost-related reasons often determine this choice, although design models are unfit for safety analysis. Design models provide limited support to safety analysis, because they are tailored for system designers. The definition of an adequate model and of an underlying methodology for its construction will be highly beneficial for performing its safety analyses. Currently, the model definition phase cannot be properly addressed as an integral part of safety analysis, mostly, due to limited costs and resources. This paper introduces a framework that support evolutionary safety analysis. The proposed framework addresses three main points in order effectively to support evolutionary safety analysis and to capture emerging complex interactions.

Firstly, the model questions the system boundaries and the required level of details. These aspects considerably vary from design models to risk analysis models, since system parts that need to be specified in details for the design may be much less relevant from a safety point of view. The typical drawback experienced in most cases is that resources for risk analysis may be consumed in investigating detailed aspects of every system part, instead of trying to identify unknown hazards that may be related to elements not central in the design model. Furthermore, it is often the case that system boundaries can be more neatly defined with respect to the design objectives, whilst risk analysis often requires the adoption of a wide focus. Most recent major incidents occurred in the civil aviation domain proved to stem from unexpected interactions from a large variety of elements [36], differently located in space and time. Those elements were often judged as outside of the system boundaries (or outside of normal operating conditions) when safety analysis has been conducted. For instance, the investigation report [8] of the accident between two aircrafts highlights that although individual ATM systems and procedures work properly, the ATM socio-technical interactions may, unfortunately, result in a catastrophic event. The iterative nature of the framework allows the gathering of emerging information. In particular, the framework captures how safety cases evolve in order to accommodate arising safety problems. The safety space transformation identifies the safety case construction and judgement in terms of safety argumentations and constraints. The safety case consists of the collections of mappings between safety cases and problems. The first part of a safety case consists of the safety argumentations, which capture the relationship that comes from safety cases looking for problems. The second part of a safety case consists of the safety constraints, which capture how future safety cases address given problems. The definition of safety case transformation enables us further to interpret and understand safety case changes, hence safety case evolution. Therefore, the framework enables the implementation of evolutionary safety analysis [6].

The second point directly addresses unexpected complex interactions between system elements as main source of incidents. Best practices and standards in safety analysis prescribe that mutual impact between different hazards to be analysed. A system model is a key support to perform this task effectively, but the possible interactions need to be represented explicitly. On the contrary, models defined for design purposes usually outline the relationship between system elements by a functional (or physical) decomposition. Although it is possible to exploit design models for safety analysis [56,57], the functional decomposition principle may unduly provide the structure for the analysis of incident causal dynamics [46,58], thus failing to acknowledge their different underlying nature.

Furthermore, a correct model should ensure that interactions and mutual impact between different risks to be analysed. Moreover, it should also outline interactions between everyday productive processes in "normal operating conditions", since risk factors are likely to interact along these lines.

The third characteristic of the model refers to the possibility of effective re-use of (part of) the model to inform other safety analyses. The framework relies on basic logic models (i.e., Kripke models) that enable reasoning about knowledge [59] and uncertainty [60]. This highlights safety judgement (that is, the construction of safety cases) as an organisational process. That is, the safety judgement consists of gathering organisational knowledge about the system. This further highlights how organisational (knowledge) failures affect safety [4,16,25]. This would ensure that part of the safety feedback and experience related to a system can be beneficial when introducing major changes to the current system or when developing new similar systems. Similarly, the effective reuse of the model would result in safety analyses that have better means to achieve a good balance between exhaustiveness and cost, as findings of closely related analysis could be easily considered.

In conclusion, this paper is concerned with problems in modelling ATM systems for evolutionary safety analysis. The main objective is to highlight a model specifically targeted to support evolutionary safety analysis of ATM systems. Moreover, the systematic production of safety analysis (models) will decrease the cost of conducting safety analyses by supporting reuse in future ATM projects.

References

[1] EUROCONTROL. EUROCONTROL air traffic management strategy for the years 2000+; 2003.

[2] Matthews S. Future developments and challenges in aviation safety. Flight Saf Dig 2002;21(11):1–12.

[3] Overall M. New pressures on aviation safety challenge safety management systems. Flight Saf Dig 1995;14(3):1–6.

[4] Leveson NG. SAFEWARE: system safety and computers. Reading, MA: Addison-Wesley; 1995.

[5] Storey N. Safety-critical computer systems. Reading, MA: Addison-Wesley; 1996.

[6] Felici M. Evolutionary safety analysis: motivations from the air traffic management domain. In: Winther R, Gran B, Dahll G, editors. Proceedings of the 24th international conference on computer safety, reliability and security, SAFECOMP 2005. Lecture Notes in Computer Science, vol. 3688. Berlin: Springer; 2005. p. 208–21.

[7] EUROCONTROL. EUROCONTROL safety regulatory requirements (ESARR). ESARR 4—risk assessment and mitigation in ATM. 1st ed.; 2001.

[8] BFU. Investigation report, AX001-1-2/02; 2002.

[9] Review, Working towards a fully interoperable system: the EUROCONTROL overall ATM/CNS target architecture project (OATA). Skyway 2004;32:46–7.

[10] Laprie J-C, et al. Dependability handbook. Technical report LAAS report no 98-346, LIS LAAS-CNRS; August 1998.

[11] EUROCONTROL. EUROCONTROL airspace strategy for the ECAC states, ASM.ET1.ST03.4000-EAS-01-00. 1st ed.; 2001.

[12] Ranter H. Airliner accident statistics 2002: statistical summary of fatal multi-engine airliner accidents in 2002. Technical report, Aviation Safety Network; January 2003.

[13] Ranter H. Airliner accident statistics 2003: statistical summary of fatal multi-engine airliner accidents in 2003. Technical report, Aviation Safety Network; January 2004.

[14] van Es GW. A review of civil aviation accidents—air traffic management related accident: 1980–1999. In: Proceedings of the fourth international air traffic management R&D seminar, New-Mexico; 2001.

[15] Enders JH, Dodd RS, Fickeisen F. Continuing airworthiness risk evaluation (CAPE): an exploratory study. Flight Saf Dig 1999;18(9–10):1–51.

[16] Perrow C. Normal accidents: living with high-risk technologies. Princeton, NJ: Princeton University Press; 1999.

[17] EUROCONTROL. EUROCONTROL air navigation system safety assessment methodology. 2nd ed.; 2004.

[18] Johnson C. Final report: review of the BFU Überlingen accident report, version 1:17/12/2004, contract C/1.369/HQ/SS/04. Technical report, EUROCONTROL; 2004.

[19] Flight safety foundation. The human factors implications for flight safety of recent developments in the airline industry. Flight Saf Dig 2003;22(3–4).

[20] Pasquini A, Pozzi S. Evaluation of air traffic management procedures—safety assessment in an experimental environment. Reliab Eng Syst Safety 2005;89(1):105–17.

[21] Wright PC, Fields RE, Harrison MD. Analysing human–computer interaction as distributed cognition: the resources model. Human Comput Interact 2000;15(1):1–41.

[22] Filipe JK, Felici M, Anderson S. Timed knowledge-based modelling and analysis: on the dependability of socio-technical systems. In: HAAMAHA 2003. Eighth international conference on human aspects of advanced manufacturing: agility & hybrid automation, ISBN 88-85059-14-7, Rome, Italy; 2003. p. 321–8.

[23] Johnson CW, Holloway CM. On the over-emphasis of human 'error' as a cause of aviation accidents: 'systemic failures' and 'human erro' in US NTSB and Canadian TSB aviation reports; 2005.

[24] Hollnagel E. Human reliability analysis: context and control. New York: Academic Press; 1993.

[25] Reason J. Managing the risks of organizational accidents. Ashgate Publishing Limited; 1997.

[26] Johnson CW. Looking beyond the cockpit: human computer interaction in the causal complexes of aviation accidents. In: HCI in aerospace 2004, EURISCO, Toulouse, France; 2004. p. 17–24.

[27] Norman DA. The invisible computer. Cambridge, MA: The MIT Press; 1998.

[28] Paternò F, Santoro C, Tahmassebi S. The impact of different media on safety and usability of interactive atc applications. In: Felici M, Kanoun K, Pasquini A, editors. Proceedings of the 18th international conference on computer safety, reliability and security, SAFECOMP 1999. Lecture Notes in Computer Science, vol. 1698. Berlin: Springer; 1999. p. 89–102.

[29] Rognin L, Blanquart J-P. Impact of communication on systems dependability: human factors perspectives. In: Felici M, Kanoun K, Pasquini A, editors. Proceedings of the 18th international conference on computer safety, reliability and security, SAFECOMP 1999. Lecture Notes in Computer Science, vol. 1698. Berlin: Springer; 1999. p. 113–24.

[30] Rognin L, Blanquart J-P. Human communications, mutual awareness and system dependability lessons learnt from air-traffic control filed studies. Reliab Eng & Syst Saf 2001;71(3):327–36.

[31] Edwards E. Man and machine: systems for safety. In: Proceedings of British airline Pilots Associations technical symposium, British Airline Pilots Associations, London; 1972. p. 21–36.

[32] Rushby J. Using model checking to help discover mode confusions and other automation surprises. Reliab Eng Syst Saf 2002;75(2): 167–77.

[33] Anderson S, Felici M. Heterogeneous modelling of evolution for socio-technical systems. In: Supplemental volume of the 2004 international conference on dependable systems and networks, workshop on interdisciplinary approaches to achieving and analysing system dependability; 2004. p. 210–5.

[34] Honeywell, TCAS II/ACAS II. Collision Avoidance System User's Manual. ACS-5059 Rev.-5-02/2000; 2000.

[35] Douglas M, Wildavsky A. Risk and culture: an essay on the selection of technological and environmental dangers. University of California Press; 1982.

[36] Knight JC. Software challenges in aviation systems. In: Anderson S, Bologna S, Felici M, editors. Proceedings of the 21st international conference on computer safety, reliability and security, SAFECOMP 2002. Lecture Notes in Computer Science, vol. 2434. Berlin: Springer; 2002. p. 106–12.

[37] Hughes AC, Hughes TP., editors. Systems, experts, and computers: the systems approach in management and engineering. World War II and after. Cambridge, MA: The MIT Press; 2000.

[38] Heitmeyer CL. Software cost reduction. In: Marciniak JJ., editor. Encyclopedia of software engineering. 2nd ed. New York; Wiley; 2002.

[39] Hoffman DM, Weiss DM., editors. Software fundamentals: collected papers by David L. Parnas. Reading, MA: Addison-Wesley; 2001.

[40] Leveson NG. Intent specifications: an approach to building human-centered specifications. IEEE Trans Software Eng 2000;26(1):15–35.

[41] MacKenzie DA. Inventing accuracy: a historical sociology of nuclear missile guidance. Cambridge, MA: The MIT Press; 1990.

[42] MacKenzie DA, Wajcman J., editors. The social shaping of technology. 2nd ed. Open University Press; 1999.

[43] Bergman M, King JL, Lyytinen K. Large-scale requirements analysis as heterogeneous engineering, Social Thinking—Software Practice 2002; 357–86.

[44] Bergman M, King JL, Lyytinen K. Large-scale requirements analysis revisited: the need for understanding the political ecology of requirements engineering. Requir Eng 2002;7(3):152–71.

[45] Felici M. Observational models of requirements evolution. Ph.D. thesis, Laboratory for Foundations of Computer Science, School of Informatics, The University of Edinburgh; 2004.

[46] Johnson CW. Failure in safety-critical systems: a handbook of accident and incident reporting. Glasgow, Scotland: University of Glasgow Press; 2003.

[47] Greenwell WS, Strunk EA, Knight JC. Failure analysis and the safety-case lifecycle. In: Proceedings of the IFIP working conference on human error, safety and system development (HESSD). New York: Wiley; 2004. p. 163–76.

[48] Kelly TP. Arguing safety—a systematic approach to managing safety cases. Ph.D. thesis, Department of Computer Science, University of York; 1998.

[49] Kelly TP, McDermid JA. A systematic approach to safety case maintenance. In: Felici M, Kanoun K, Pasquini A, editors. Proceedings of the 18th international conference on computer safety, reliability and security, SAFECOMP'99. Lecture Notes in Computer Science, vol. 1698. Berlin: Springer; 1999. p. 13–26.

[50] Kelly TP, McDermid JA. A systematic approach to safety case maintenance. Reliab Eng Syst Saf 2001;71(3):271–84.

[51] Aviation Safety Reporting System, Controller Reports; 2003.

[52] Aviation Safety Reporting System, TCAS II Incidents; 2004.

[53] Shappell SA, Wiegmann DA. The human factors analysis and classification system—HFACS. Technical report DOT/FAA/AM-00/7, FAA; February 2000.

[54] Wiegmann DA, Shappell SA. A human error analysis of commercial aviation accidents using the human factors analysis and classification system (HFACS). Technical report DOT/FAA/AM-01/3, FAA; February 2001.

[55] Hollnagel E. The art of efficient man–machine interaction: improving the coupling between man and machine. In: Expertise and technology: cognition & human–computer cooperation. Lawrence Erlbaum Associates; 1995. p. 229–41.

[56] Bate I, Kelly T. Architectural considerations in the certification of modular systems. In: Anderson S, Bologna S, Felici M, editors. Proceedings of the 21st international conference on computer safety, reliability and security, SAFECOMP 2002. Lecture Notes in Computer Science, vol. 2434. Berlin: Springer; 2002. p. 321–33.

[57] Bate I, Kelly T. Architectural considerations in the certification of modular systems. Reliab Eng Syst Saf 2003;81(3):303–24.

[58] Leveson N. A new accident model for engineering safer systems. Safety Sci 2004;42(4):237–70.

[59] Fagin R, Halpern JY, Moses Y, Vardi MY. Reasoning about knowledge. Cambridge, MA: The MIT Press; 2003.

[60] Halpern JY. Reasoning about uncertainty. Cambridge, MA: The MIT Press; 2003.