Evolutionary Safety Analysis: Motivations from the Air Traffic Management Domain

Massimo Felici

LFCS, School of Informatics, The University of Edinburgh, Edinburgh EH9 3JZ, UK
mfelici@inf.ed.ac.uk
http://homepages.inf.ed.ac.uk/mfelici/

Abstract. In order realistically and cost-effectively to realize the ATM (Air Traffic Management) 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). 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 whom is performing safety analyses. Limited budgets and resources, often, constrain or inhibit the model definition phase as an integral part of safety analysis. This paper is concerned with problems in modeling ATM systems for safety analysis. The main objective is to highlight a model specifically targeted to support evolutionary safety analysis.

1 Introduction

The future development of Air Traffic Management (ATM), set by the ATM 2000+ Strategy [9], involves a structural revision of ATM processes, a new ATM concept and a systems approach for the ATM network. The overall objective [9] 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 the cost-effectively gaining of extra capacity together with the increase of safety levels [28,29]. Enhancing safety levels affects the ability to accommodate increased

R. Winther, B.A. Gran, and G. Dahll (Eds.): SAFECOMP 2005, LNCS 3688, pp. 208–221, 2005.

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 foreseen 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 [24,37].

Diverse domains (e.g., nuclear, chemical or transportation) adopt safety analyses that originate from a general approach [24,37]. 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 [8]. Unfortunately, ATM systems and procedures have distinct characteristics[1] (e.g., openness, volatility, etc.) that expose limitations of the approach. In particular, the complete identification of the system under analysis [22] 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 the unproblematic application of conventional safety analysis. Physical design structures constrain system interactions and stress the separation of safety related components from other system parts. This ensures the independence of failures. By contrast, ATM systems operate in open and dynamic environments where it is difficult completely to identify system interactions. For instance, there exist *complex interactions*[2] between aircraft systems and ATM safety relevant systems [31]. Unfortunately, these complex interactions may give rise to catastrophic failures. The accident (1 July 2002) between a BOEING B757-200 and a Tupolev TU154M [5], 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 [5]. 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.

This paper is concerned with limitations of safety analysis with respect to evolution. The paper is structured as follows. Section 2 describes safety analysis

[1] *"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."*, p. 123, [31].

[2] *"Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible."*, p. 78, [31].

in the ATM domain. Unfortunately, ATM systems, procedures and interactions expose limitations of safety analysis. Section 3 proposes a framework that enhances evolutionary safety analysis. Section 4, finally, 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 [9]. Currently, ATM services are going through a structural revision of processes, systems and underlying ATM concepts. This highlights a systems approach for the ATM network. The delivery and deployment of new systems will let a new ATM architecture to emerge. The EUROCONTROL OATA project [35] 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 [23] 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 [7]. 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 [32,33,38]. Many relevant repositories[3] 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 [6].

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 [8], ESARR4,

[3] 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/ -.

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 [8] 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) [10] reflecting best practices for safety assessment of Air Navigation Systems.

The SAM methodology provides a means of compliance to ESARR4. The SAM methodology describes a generic process for the safety assessment of Air Navigation Systems. The objective of the methodology is to define the means for providing assurance that an Air Navigation System is safe for operational use. The 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)*. Figure 1 shows how the SAM methodology contributes towards system assurance.

The process covers the complete lifecycle of an Air Navigation System, from initial system definition, through design, implementation, integration, transfer to operations and maintenance. Although the SAM methodology describes the underlying principles of the safety assessment process, it provides limited information to applying these principles in specific projects. 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.

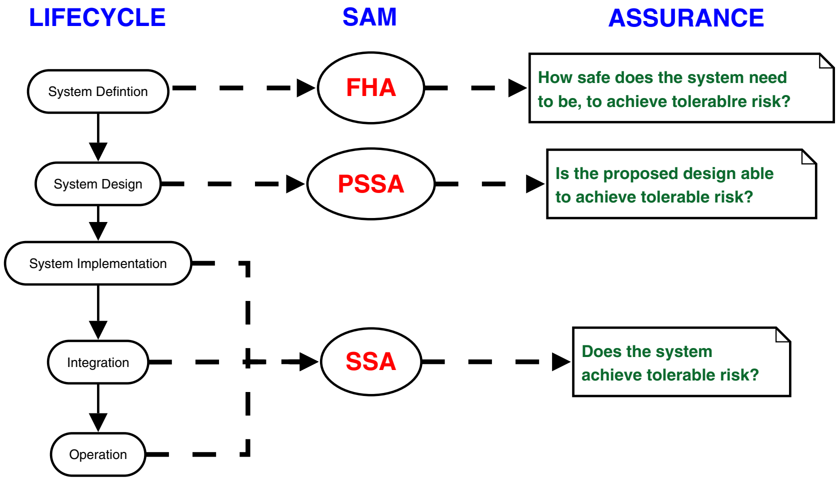
LIFECYCLE
SAM
ASSURANCE
System Defintion
FHA
How safe does the system need to be, to achieve tolerablre risk?
System Design
PSSA
Is the proposed design able to achieve tolerable risk?
System Implementation
Integration
SSA
Does the system achieve tolerable risk?
Operation

Fig. 1. Contribution of the Safety Assessment Methodology towards system assurance

2.1 Limitations

Conventional safety analysis is 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. By 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 and ATM safety functions. Unfortunately, this complex interaction may give rise to catastrophic failures. Hence, failure independence would increase the overall ATM safety.
- Humans [12,30] 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 artifacts (e.g., tools) to mediate this interaction. This would allow the understanding of how humans adopt technological artifacts 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 would allow the modeling of evolution. This will enhance strategies for deploying new system configurations or major system upgrades. On the one hand, modeling and understanding system evolution support the engineering of (evolving) ATM systems. On the other hand, modeling and understating 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 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. Figure 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 Modeling Transformation (SMT)*, *Safety Analysis Modeling Transformation (SAMT)* and *Operational Modeling Transformation (OMT)*. The remainder of this section describes the three hierarchical layers.

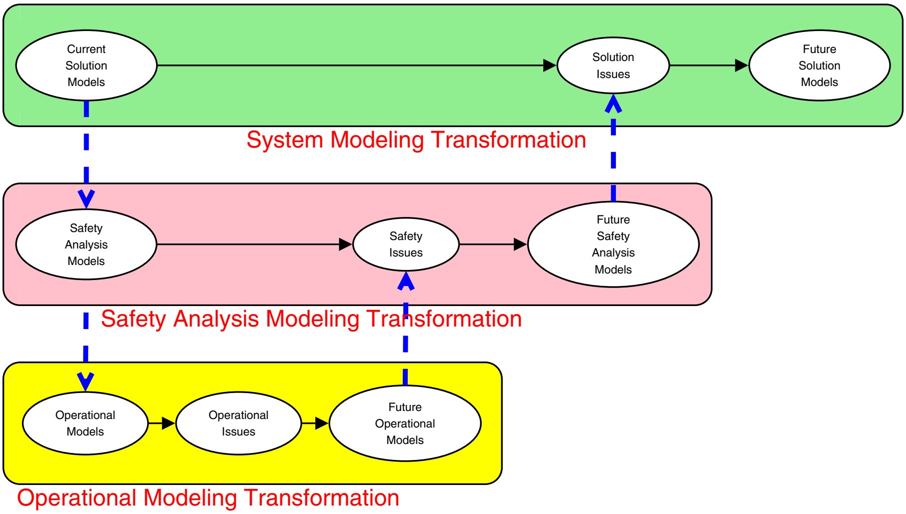
Current Solution Models
Solution Issues
Future Solution Models
System Modeling Transformation
Safety Analysis Models
Safety Issues
Future Safety Analysis Models
Safety Analysis Modeling Transformation
Operational Models
Operational Issues
Future Operational Models
Operational Modeling Transformation

Fig. 2. A framework for modelling evolutionary safety analyses

3.1 System Modeling 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. Organizational 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.

Modeling methodologies and languages advocate different design strategies. Although these strategies support different aspects of software development, they originate in a common *Systems Approach*[4] to solving complex problems and managing complex systems. Modeling incorporates design concepts and formalities into system specifications. This enhances our ability to assess safety

[4] *"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 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."*, INTRODUCTION, p. 3, [18].

requirements. For instance, *Software Cost Reduction* (SCR) consists of a set of techniques for designing software systems [14,15]. 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 modeling that further supports the analysis and design of evolving systems [25]. 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[5].

Heterogeneous engineering[6] 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 [18] as well as the social shaping of technology [27]. According to heterogeneous engineering, system requirements specify mappings between problem and solution spaces [3,4]. Both spaces are socially constructed and negotiated through sequences of mappings between solution spaces and problem spaces [3,4]. 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 [3,4,11]. 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.) [11].

System Modeling Transformation 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

[5] Leveson in [25] 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."*

[6] "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.", p. 28, [26].

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 methodology [10]. 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.

3.2 Safety Analysis Modeling Transformation

The failure of safety-critical systems highlights safety issues [19,24,31,37]. 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 [13]. Figure 3 shows an enhanced safety-case lyfecyle [13].

The lifecycle identifies a general process for the revision of safety cases. Greenwell, Strunk and Knight in [13] motivate the safety-case lifecycle by evolutionary (safety-case) examples drawn from the aviation domain. Figure 4 and 5 show subsequent versions of a safety case. The graphical notation that represents the safety

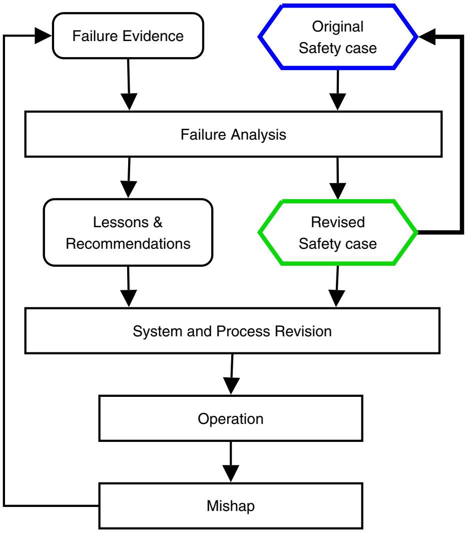

Fig. 3. The Enhanced Safety-Case Lyfecyle [13]

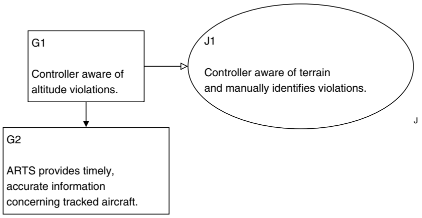
G1
Controller aware of altitude violations.
J1
Controller aware of terrain and manually identifies violations.
J
G2
ARTS provides timely, accurate information concerning tracked aircraft.

Fig. 4. Initial safety argument

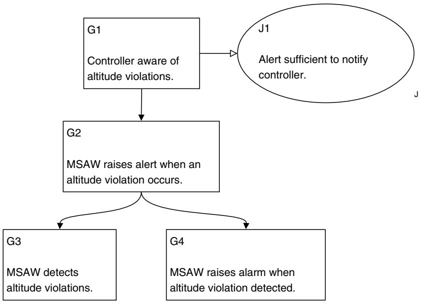
G1
Controller aware of altitude violations.
J1
Alert sufficient to notify controller.
J
G2
MSAW raises alert when an altitude violation occurs.
G3
MSAW detects altitude violations.
G4
MSAW raises alarm when altitude violation detected.

Fig. 5. Revised safety argument

cases is the Goal Structuring Notation (GSN) [21]. 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) [20]. Moreover, it lacks any interpretation of the relationships between subsequent safety cases.

Figure 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. Figure 5 shows the revised safety case that addresses the issue occurred. Unfortunately, another accident, again, invalidates the second safety case [13]. Hence, the safety argument needs further revision in order to address the safety flaw uncovered by the accident.

Figure 6 shows a safety space transformation that captures the safety case changes [11]. The safety case transformation captures the changes from the initial safety case $\mathcal{M}_i^t$ (see, Figure 4) to the revised safety case $\mathcal{M}_i^{t+1}$ (see, Figure 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, $\mathcal{P}_t$, 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 $\mathcal{M}_i^{t+1}$. In order to address the highlighted problems, it is necessary to change the initial safety case. 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 proble 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 [11].

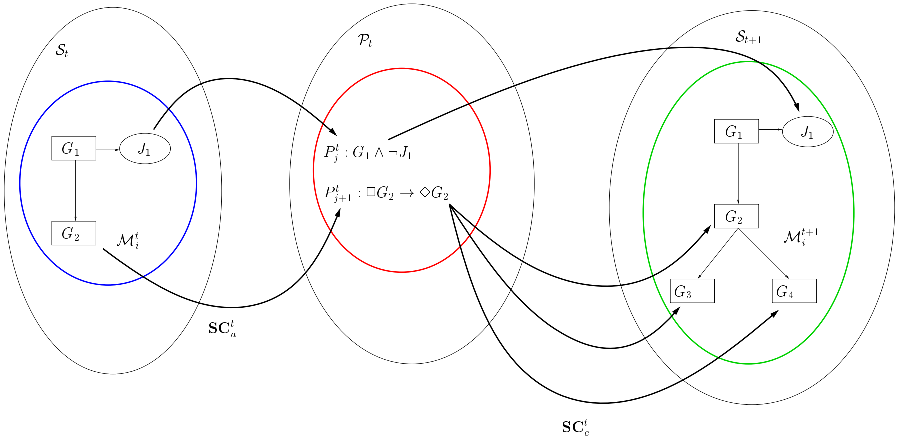

Fig. 6. A safety space transformation

Safety Analysis Modeling Transformation 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 [10]. Note that although the SAM methodology stresses that both FHA and PSSA are iterative process, it provides little supports to manage process iterations as well as system evolution in terms of design solution and safety requirements. The framework supports these evolutionary processes.

3.3 Operational Modeling 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 1 shows the main problems areas identified in reported incidents: Controller Reports [1] and TCAS II Incidents [2]. Both reports consist of the fifty 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 [31]. The analysis of the reports is in agreement with other studies [36,39] that analyse human errors as organizational failures [16,24,34].

Technically, operational observations are reported anomalies (or faults), which may trigger errors eventually resulting in failures. These observations capture *erroneous actions* [16]: *"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

Table 1. The main problem areas occuring 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

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 [16]. In a continuosly changing enviroment like ATM, adaption enhances the coupling between man and machine [17]. Hollnagel in [17] identifies three different adaption strategies: *Adaption Through Design*, *Adaption through Performance* and *Adaption through Management*. Operational Modeling Transformation 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.

4 Conclusions

This paper is concerned with problems in modeling ATM systems for safety analysis. The future development of ATM, set by the ATM 2000+ Strategy [9], 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. Evolutionary safety analysis captures the judgement of changes. Moreover, it supports the safety assessment of changes from system as well as organisation[7] viewpoints [22,24,34]. Industry (e.g., SMEs) will be involved as early as possible in the lifecycle of ATM projects. The ATM lifecycle

[7] *"Change within an organisation can affect level of safety achieved by that organisation. Change in the institutional structure of an industry can affect the level of safety achieved by the industry as a whole."*, p. 6, [22].

involves various stakeholders (e.g., Institutional, Solution Providers, Society and Other Industries) [22] assuming different roles with respect to safety judgement. Unclear responsibilities and ownerships, with respect to safety cases, affect the trustworthiness of safety analysis [22]. Evolutionary safety analysis, therefore, requires the identification of responsibilities and ownerships in order to address institutional issues (e.g., institutional changes, inappropriate ownerships, etc.).

In conclusion, this paper introduces a framework that supports evolutionary safety analysis. Although existing processes emphasise the iterative nature of safety analysis, they provide limited support to capture evolutionary transformations. The framework captures evolutionary safety analysis. Examples drawn from the ATM domain show the different relationships between subsequent evolutionary models. The systematic production of safety analysis (models) will decrease the cost of conducting safety analysis by supporting reuse in future ATM projects.

Acknowledgements. This work has been supported by the UK EPSRC Interdisciplinary Research Collaboration in Dependability, DIRC - http://www.dirc.org.uk - grant GR/N13999.

References

1. Aviation Safety Reporting System. *Controller Reports*, 2003.
2. Aviation Safety Reporting System. *TCAS II Incidents*, 2004.
3. Mark Bergman, John Leslie King, and Kalle Lyytinen. Large-scale requirements analysis as heterogeneous engineering. *Social Thinking - Software Practice*, pages 357–386, 2002.
4. Mark Bergman, John Leslie King, and Kalle Lyytinen. Large-scale requirements analysis revisited: The need for understanding the political ecology of requirements engineering. *Requirements Engineering*, 7(3):152–171, 2002.
5. BFU. *Investigation Report, AX001-1-2/02*, 2002.
6. John H. Enders, Robert S. Dodd, and Frank Fickeisen. Continuing airworthiness risk evaluation (CARE): An exploratory study. *Flight Safety Digest*, 18(9-10):1–51, September-October 1999.
7. EUROCONTROL. *EUROCONTROL Airspace Strategy for the ECAC States, ASM.ET1.ST03.4000-EAS-01-00*, 1.0 edition, 2001.
8. EUROCONTROL. *EUROCONTROL Safety Regulatory Requirements (ESARR). ESARR 4 - Risk Assessment and Mitigation in ATM*, 1.0 edition, 2001.
9. EUROCONTROL. *EUROCONTROL Air Traffic Management Strategy for the years 2000+*, 2003.
10. EUROCONTROL. *EUROCONTROL Air Navigation System Safety Assessment Methodology*, 2.0 edition, 2004.
11. Massimo Felici. *Observational Models of Requirements Evolution.* PhD thesis, Laboratory for Foundations of Computer Science, School of Informatics, The University of Edinburgh, 2004.
12. Flight Safety Fundation. *The Human Factors Inplication for Flight Safety of Recent Developments In the Airline Industry*, number (22)3-4 in Flight Safety Digest, March-April 2003.

13. William S. Greenwell, Elisabeth A. Strunk, and John C. Knight. Failure analysis and the safety-case lifecycle. In *Proceedings of the IFIP Working Conference on Human Error, Safety and System Development (HESSD)*, pages 163–176, 2004.
14. Constance L. Heitmeyer. Software cost reduction. In John J. Marciniak, editor, *Encyclopedia of Software Engineering*. John Waley & Sons, 2nd edition, 2002.
15. Daniel M. Hoffman and David M. Weiss, editors. *Software Fundamentals: Collected Papers by David L. Parnas*. Addison-Wesley, 2001.
16. Erik Hollnagel. *Human Reliability Analysis: Context and Control*. Academic Press, 1993.
17. Erik Hollnagel. The art of efficient man-machine interaction: Improving the coupling between man and machine. In *Expertise and Technology: Cognition & Human-Computer Cooperation*, pages 229–241. Lawrence Erlbaum Associates, 1995.
18. Agatha C. Hughes and Thomas P. Hughes, editors. *Systems, Experts, and Computers: The Systems Approach in Management and Engineering, World War II and After*. The MIT Press, 2000.
19. Chris W. Johnson. *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. University of Glasgow Press, Glasgow, Scotland, October 2003.
20. T. P. Kelly and J. A. McDermid. A systematic approach to safety case maintenance. In Massimo Felici, Karama Kanoun, and Alberto Pasquini, editors, *Proceedings of the 18th International Conference on Computer Safety, Reliability and Security, SAFECOMP'99*, number 1698 in LNCS, pages 13–26. Springer-Verlag, 1999.
21. Timothy Patrik Kelly. *Arguing Safety - A Systematic Approach to Managing Safety Cases*. PhD thesis, Department of Computer Science, University of York, 1998.
22. Steve Kinnersly. Whole airspace atm system safety case - preliminary study. Technical Report AEAT LD76008/2 Issue 1, AEA Technology, 2001.
23. Jean-Claude Laprie et al. Dependability handbook. Technical Report LAAS Report no 98-346, LIS LAAS-CNRS, August 1998.
24. Nancy G. Leveson. *SAFEWARE: System Safety and Computers*. Addison-Wesley, 1995.
25. Nancy G. Leveson. Intent specifications: An approach to building human-centered specifications. *IEEE Transactions on Software Engineering*, 26(1):15–35, January 2000.
26. Donald A. MacKenzie. *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*. The MIT Press, 1990.
27. Donald A. MacKenzie and Judy Wajcman, editors. *The Social Shaping of Technology*. Open University Press, 2nd edition, 1999.
28. Stuart Matthews. Future developments and challenges in aviation safety. *Flight Safety Digest*, 21(11):1–12, November 2002.
29. Michael Overall. New pressures on aviation safety challenge safety management systems. *Flight Safety Digest*, 14(3):1–6, March 1995.
30. Alberto Pasquini and Simone Pozzi. Evaluation of air traffic management procedures - safety assessment in an experimental environment. *Reliability Engineering & System Safety*, 89(1):105–117, July 2005.
31. Charles Perrow. *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press, 1999.
32. Harro Ranter. Airliner accident statistics 2002: Statistical summary of fatal multi-engine airliner accidents in 2002. Technical report, Aviation Safety Network, January 2003.

33. Harro Ranter. Airliner accident statistics 2003: Statistical summary of fatal multi-engine airliner accidents in 2003. Technical report, Aviation Safety Network, January 2004.
34. James Reason. *Managing the Risks of Organizational Accidents.* Ashgate Publishing Limited, 1997.
35. Review. Working towards a fully interoperable system: The EUROCONTROL overall ATM/CNS target architecture project (OATA). *Skyway*, 32:46–47, Spring 2004.
36. Scott A. Shappell and Douglas A. Wiegmann. The human factors analysis and classification system - HFACS. Technical Report DOT/FAA/AM-00/7, FAA, February 2000.
37. Neil Storey. *Safety-Critical Computer Systems.* Addison-Wesley, 1996.
38. Gerard W.H. van Es. A review of civil aviation accidents - air traffic management related accident: 1980-1999. In *Proceedings of the 4th International Air Traffic Management R&D Seminar*, New-Mexico, December 2001.
39. Douglas A. Wiegmann and Scott A. Shappell. 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.