Evolutionary Risk Analysis: Expert Judgement

Massimo Felici[1], Valentino Meduri[1],
Bjørnar Solhaug[2], and Alessandra Tedeschi[1,⋆]

[1] Deep Blue S.r.l.
Piazza Buenos Aires 20, 00198 Roma, Italy
alessandra.tedeschi@dblue.it
http://www.dblue.it/
[2] SINTEF ICT
P.O. Box 124 Blindern, 0314 Oslo, Norway

Abstract. New systems and functionalities are continuously deployed in complex domains such as Air Traffic Management (ATM). Unfortunately, methodologies provide limited support in order to deal with changes and to assess their impacts on critical features (e.g. safety, security, etc.). This paper is concerned with how change requirements affect security properties. A change requirement is a specification of changes that are to be implemented in a system. The paper reports our experience to support an evolutionary risk analysis in order to assess change requirements and their impacts on security properties. In particular, this paper discusses how changes to structured risk analysis models are perceived by domain experts by presenting insights from a risk assessment exercise that uses the CORAS model-driven risk analysis in an ATM case study. It discusses how structured models supporting risk analysis help domain experts to analyse and assess the impact of changes on critical system features.

Keywords: Air Traffic Management, Change Requirements, Security Requirements, Evolutionary Risk Analysis, CORAS.

1 Changes and Risks

Standards, guidelines and best practices advise to assess the impact of changes. In safety-critical contexts, or other domains characterised by stringent critical non-functional requirements (e.g. reliability, security, safety), it is necessary to assess how changes affect system properties. This aspect concerns system artifacts at any developmental stage. For instance, safety cases need to be adapted in order to take into account any emergent system knowledge (e.g. system failures), system requirements need to change in order to accommodate evolving environmental factors, testing activities need to be performed again in order to assess software and configuration changes. Similarly, risk analysis needs to take into account changes and emergent hazards because changes and evolution may affect the risk picture. On the one hand, changes and evolution may introduce new or

[⋆] Corresponding author.

F. Flammini, S. Bologna, and V. Vittorini (Eds.): SAFECOMP 2011, LNCS 6894, pp. 99–112, 2011.

different threats and stress system vulnerabilities. On the other hand, changes and evolution may provide opportunities for enhancing system dependability.

Unfortunately, support throughout the system lifecycle for systematically dealing with changes and evolution is patchy. Recent research (e.g. see [18, 19, 24, 25, 26] for work concerned in particular with the AMT domain) highlights some challenges for risk assessment methodologies. This paper is concerned with challenges for current risk assessment methodologies in dealing with changes in particular for safety-critical domains such as ATM. It discusses an evolutionary risk analysis by means of structured models. Changes may affect various system artifacts (e.g. requirements, design models). They require such artifacts to be updated and reassessed eventually. This inevitably increases project costs associated with maintaining a valid risk assessment for the system. It may affect reusing strategies as well as any effort to localise changes into specific arguments (hence, increasing intrinsic system complexities). However, although different structured models (e.g. design models, risk models, safety arguments, etc.) are used to support risk analysis, this paper is concerned with whether structured models provide suitable support in order to acquire expert judgement while risk analysis deals with changes — *How do models support assessing the impact of changes? How do changes into models shift risk perception?* This paper reports our experience of evolutionary risk analysis supported by the CORAS approach. Section 2 reviews relevant work on risk analysis, and highlights guidelines and methodologies drawn from the ATM domain. Section 3 describes a case study drawn from ongoing activities within the ATM domain. Section 4 introduces the basic concepts of the CORAS approach to model-driven risk analysis. Section 5 reports our evolutionary risk analysis and the investigation results taking into account expert judgements during dedicated risk analysis sessions. Section 6 summarises our lessons learned.

2 Related Work on Risk Analysis

The ISO 31000 risk management standard [1] defines risk management as coordinated activities to direct and control an organisation with regard to risk, where risk can be understood as the combination of the likelihood and consequence of an unwanted incident. The risk management process includes the phases of context establishment, risk assessment and risk treatment. Context establishment involves defining the target of analysis and setting the risk criteria, whereas risk assessment involves risk identification, risk analysis and risk evaluation. The risk analysis estimates the likelihoods and consequences of risks, and the risk evaluation compares the resulting risk levels with the criteria in order to determine which risks must be mitigated by treatment options. The ISO 31000 standard stresses the importance of handling changes. However, the standard comes with no explicit guidelines for how to manage and assess changing risks. Other established risk analysis methods such as OCTAVE [2] and CRAMM [3, 4] follow a process similar to ISO 31000. Such methods focus on a particular configuration of the target at a particular point in time, and the results are therefore valid only for this particular snapshot and for the assumptions being made. When addressing changing systems, there is a need for risk analysis methods that comes with guidelines and techniques for how to understand, to assess and to document risks as changing risks. There is a need for risk modelling techniques to facilitate the tasks of assessing changing risks. Structured risk models represent unwanted incidents with their causes and consequences by graphs (e.g. Cause-consequence analysis and Bayesian networks [9]), trees (e.g. Fault Tree Analysis [6], Event Tree Analysis [7] and Attack trees [8]) or block diagrams [5].

CORAS threat diagrams [11] describe how threats exploit vulnerabilities to initiate threat scenarios and unwanted incidents, as well as the likelihoods and consequences of incidents. Risks graphs represent an abstraction of each of the above mentioned risk modelling techniques in the sense that each of them can be understood as a risk graph instantiation [12]. Risk graphs facilitate the structuring of events that lead to incidents, as well as the estimation of likelihoods. The notation is provided a formal semantics and comes with a calculus for reasoning about likelihoods. Unfortunately, risk modelling techniques provide limited support for the identification, modelling and assessment of changing risks. This paper presents an evolutionary risk analysis that generalises the risk graph notation in order to support the modelling of risks that evolve. This generalisation is in turn instantiated in CORAS, thus supporting a CORAS risk analysis process with methods and techniques for assessing and documenting evolving risks.

The risk associated with the *high-couple* and *complex interactions* emerging among system 'components' is characterising for many technology systems [15], in particular ATM systems. The socio-technical nature of such systems involves diverse entities interacting within operational environments. The SHEL model characterises the socio-technical nature of ATM systems and their distributed nature [16]. Causal analysis of failures in such systems highlights that failures are often *interaction* or *organisational* failures. The Cheese model provides a characterisation how failures emerge within organisations [17]. Safety mechanisms and barriers address to a certain extent threats and vulnerabilities across organisational layers [17]. Such concepts underlie safety nets in the ATM domain [20]. The EUROCONTROL Permanent Commission approved a number of ATM safety regulatory requirements, known as ESARRs, but these represent only one element of a wider framework for ATM safety regulation. These requirements are mandatory for all EUROCONTROL Member States and aim at harmonising the ATM safety regulation across the ECAC area. ECAC States not member of EUROCONTROL are strongly encouraged to adopt the ESARRs as well. EUROCONTROL, through the Safety Regulation Commission (SRC), is developing a harmonised framework for the safety regulation of ATM, for implementation by States. The core of the framework is represented by harmonised safety regulatory requirements, ESARRs. ESARR 4 (Risk Assessment and Mitigation in ATM) [21] and ESARR 6 (Software in ATM systems) [22] are of particular relevance. In order to comply with the ESARRs and to support the deployment of ATM systems, EUROCONTROL is developing the Integrated Risk Picture

Methodology (IRP) [23]. Relevant guidelines and requirements stress that risk analysis needs to deal with changes, hence, an evolutionary risk analysis.

3 ATM Case Study

In Air Traffic Management the increase of air traffic is pushing the human performances to the limit, and the level of automation is growing dramatically to deal with the need for fast decisions and high traffic load. There is an increase in data exchange between aircraft and ground and between Area Control Centers (ACCs) due to new systems, equipments and ATM strategies. There is a growing relevance for dependability, security and privacy aspects. Software and devices must adapt to evolution of processes, introduction of new services, and modification of the control procedures. This adaptation shall preserve safety, security and dependability and be able to face new and unexpected security problems arising from evolution. Introducing Safety and Security relevant methodologies in the ATM context requires us to understand the risk involved in order to mitigate the impact of possible future threats and failures. The ATM 2000+ Strategic Agenda [29] and the Single European Sky ATM Research [30] (SESAR) Initiative, involve 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 SESAR. The SESAR Operational Concept is a trajectory based system, which relies on precise trajectory data, combined with cockpit displays of surrounding traffic. The execution of such trajectory by Air Traffic Management services will ensure that traffic management is carried out safely and cost efficiently within the infrastructural and environmental constraints.

Changes to the business trajectory must be kept to a minimum. Modifications to the business trajectory are best met through maintenance of capacity and throughput rather than optimisation of an individual flight. Changes will ideally be performed through a Collaborative Decision Making mechanism but without interfering with the pilots' and controllers' tactical decision processes required for separation provision, for safety or for improvement of the air traffic flow, thanks to the new tools that will be introduced in the Controller Working Position (CWP). Sharing access to accurately predicted, business trajectories information will reduce uncertainty and give all stakeholders a common reference, permitting collaboration across all organisational boundaries.

Fundamental to the entire ATM Target Concept is a net-centric operation based on: (1) a powerful information handling network for sharing data; (2) new air-air, ground-ground and air-ground data communications systems, and; (3) an increased reliance of airborne and ground based automated support tools. The ATM case study is concerned with changes to operational processes of managing air traffic in Terminal Areas. Arrival management is a very complex process, involving different actors. Airport actors are private organisations and public authorities with different roles, responsibilities and needs. The subsequent introduction of new tools (e.g. Queue Managers) and the introduction of a new ATM network for the sharing and management of information affect the ATM system at an organisational level.

3.1 Organisational Level Change

The introduction of the AMAN (Arrival Manager) affects Controller Working Positions (CWPs) as well as the Area Control Center (ACC) environment as a whole. The main foreseen changes in the ACC from an operational and organisational point of view are the automation of tasks (i.e. the usage of the AMAN for the computation of the Arrival Sequence) that in advance were carried out by Air Traffic Controllers (ATCOs), a major involvement of the ATCOs of the upstream Sectors in the management of the inbound traffic. These changes will also require the redefinition of the Coordinator of the Arrival Sequence Role, who will be responsible for monitoring and modifying the sequences generated by the AMAN, and providing information and updates to the Sectors. The AMAN's interfaces provide access to different roles, and authorisations need to make information available only to authorised personnel or trusted systems.

3.2 Security Properties

Main aspects of security in ATM relate to self protection of facilities and resources of the ATM system as well as coordination with Air Defense authorities for exchange of information and coordination in case of aviation security incidents. The ATM is above all a cooperative system, based on mutual trust primarily between airspace users and ATM staff. Traffic surveillance relies currently on sensors that can bring additional confidence to the integrity of information received. Surveillance of traffic and monitoring of information may be used to detect civil aircraft operating in such a manner as to raise suspicion of seizure by terrorists or hijackers. The introduction of new systems and the reorganisation of ATM services are facing new security issues. Both ATM security and safety are concerned with protecting ATM assets and services, that seeks to safeguard the overall airspace from unauthorised use, intrusion or other violations. EUROCONTROL has recently issued several guidelines highlighting security as a critical factor for future ATM developments and identifying relevant security

Table 1. Security Properties

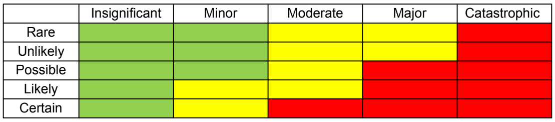
Security Property	Description
Information Protection	Unauthorised actors (or systems) are not allowed to access confidential queue management information.
Information Provision	The provisioning of information regarding queue management sensitive data by specific actors (or systems) must be guaranteed 24 hours a day, 7 days a week, taking into account the kind of data shared, their confidentiality level and the different actors involved.

methodologies [27, 28]. Table 1 identifies critical security properties to be guaranteed at the process and organisational level. Our risk analysis study focuses on such security properties.

4 Model-Driven Risk Analysis: The CORAS Approach

CORAS [11] is an approach to risk analysis that consists of three tightly integrated parts, namely the CORAS method, the CORAS language and the CORAS tool. The method is based on the ISO 31000 risk management standard [1] and consists of eight steps. The four first steps correspond to the context establishment, whereas the remaining four are risk identification, risk estimation, risk evaluation and risk treatment. The method comes with concrete tasks and practical guidelines for each step, and is supported by several risk analysis techniques. The CORAS language consists of five kinds of diagrams, each of which provides support for specific tasks throughout the whole risk assessment process. The method is supported by the tool, which is an editor for on-the-fly risk modelling. The most important kind of CORAS diagram is threat diagrams which are used for risk identification and risk estimation. The language constructs are firmly based on an underlying well-defined conceptual framework for reasoning about risk, and includes: human and non-human threats, vulnerabilities, threat scenarios, unwanted incidents and assets. Threat diagrams are used for on-the-fly risk modelling during structured brainstorming that involves personnel with expert knowledge about the target of analysis. In such a setting, the diagrams must be intuitive and easy to understand, also for people with little technical background and little experience in risk analysis. For this reason, the CORAS language constructs are graphical, easily understandable symbols. In the following we describe and exemplify selected parts of the generalised CORAS approach and the risk analysis of the ATM case study, focusing on the identification and modelling of changing risks since this is the core part of the process [13].

Context Establishment. The context establishment includes making the target description, setting the focus and scope of the analysis, identifying the assets, and setting the risk evaluation criteria. In the setting of evolving systems, the context establishment moreover includes the specification of the changes to the target, the changes in assets or asset values, and the changes to the evaluation criteria, if any. Figure 1 shows the risk evaluation criteria partially based on the EUROCONTROL safety regulatory requirement (ESARR4) [21].



	Insignificant	Minor	Moderate	Major	Catastrophic
Rare	🟩	🟩	🟨	🟨	🟥
Unlikely	🟩	🟩	🟨	🟨	🟥
Possible	🟩	🟩	🟨	🟥	🟥
Likely	🟩	🟨	🟨	🟥	🟥
Certain	🟩	🟨	🟥	🟥	🟥

Fig. 1. Risk evaluation criteria

Our target of analysis, both its structure and its behavior before and after the changes, were specified by UML 2.0 diagrams [14]. In the risk analysis, the identified assets of confidentiality and availability correspond to the security properties of Information Protection and Information Provision, respectively.

Risk Identification. The risk identification was conducted as a structured brainstorming involving personnel with first hand knowledge about the target of analysis and strong background from ATM. By conducting a walkthrough of the UML target description, the risks were identified by systematically identifying unwanted incidents, threats, threat scenarios and vulnerabilities. The results were documented by means of CORAS threat diagrams. So far, the methods and techniques are as for traditional risk analyses. However, a guiding principle for our risk analysis method generalised to handle evolving systems and risks is that only the risk analysis results that are affected by the system changes should be addressed anew. In our generalisation of CORAS we provide techniques and language support for tracing changes from the target system to the risk model so as to enable the identification of the parts of the risk models that are not affected by changes and therefore maintain their validity. Because our main concern in this paper is to present the insights from the evolutionary risk assessment case study regarding expert judgement, we refer to the full report for further details about the method and techniques [13]. Figure 2 shows a fragment of a CORAS threat diagram resulting from the identification of changing risks.

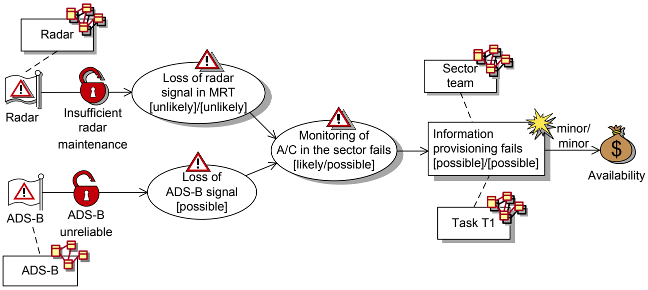
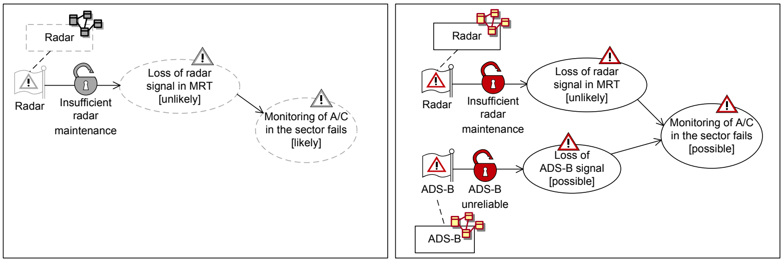

Radar
Radar
Insufficient radar maintenance
Loss of radar signal in MRT [unlikely]/[unlikely]
Monitoring of A/C in the sector fails [likely/possible]
Sector team
Information provisioning fails [possible]/[possible]
minor/ minor
Availability
ADS-B
ADS-B unreliable
Loss of ADS-B signal [possible]
Task T1
ADS-B

Fig. 2. Threat diagram with changing risks

Compared with the standard CORAS language, there are two main language extensions to support the risk analysis of evolving systems. First, the rectangle icons with the system diagram symbol (e.g. the one named Task T1 - the first task in the arrival management work process) exemplify the new construct for referring to the target of analysis. Second, the threat diagram language constructs of threat, unwanted incident, asset, etc. are generalised to three modes with different appearances, namely the modes before, after and before-after. The before constructs are in grey shade and dashed outline and represent parts of the risk picture that are valid only before the changes. The after constructs are in colour and solid outline and represent parts that are valid only after the changes.

The before-after constructs are two-layered and represent parts that are valid both before and after changes. The explicit references to the target system in the threat diagrams facilitate the identification of the parts of the risk picture that are affected by system changes. For example, in the ATM risk analysis, the radar was not subject to the ATM system changes. Hence, the vulnerability Insufficient radar maintenance and the threat scenario Loss of radar signal in MRT (multi-radar tracking) are maintained under change. The threat scenario Monitoring of A/C (aircraft) in the sector fails, on the other hand, is affected due to the introduction of the ADS-B (automatic dependent surveillance-broadcast). Notice that we take into account here the dependencies of elements on their preceding elements in the threat diagrams. The different appearance of the three modes of the language constructs facilitates the immediate recognition of the risk changes that are modelled. This feature is an important part of supporting the risk identification brainstorming and for appropriately documenting the results. In order to highlight the risk changes, the CORAS tool implements the functionality of changing between the views of before, after and before-after. Figure 3 shows such feature on an extract of the threat diagram.


Radar
Radar
Insufficient radar maintenance
Loss of radar signal in MRT [unlikely]
Monitoring of A/C in the sector fails [likely]
Radar
Radar
Insufficient radar maintenance
Loss of radar signal in MRT [unlikely]
Monitoring of A/C in the sector fails [possible]
ADS-B
ADS-B unreliable
Loss of ADS-B signal [possible]
ADS-B

(a) Before-view

(b) After-view

Fig. 3. Two views on changing risks

Risk Estimation. The risk estimation basically amounts to estimating likelihoods and consequences for unwanted incidents. Usually, we also estimate likelihoods for threat scenarios in order to get a better basis for estimating the likelihood of unwanted incidents and to understand the most important sources of risks. The CORAS calculus provides rules for calculating and reasoning about likelihoods. Diagram elements of mode before-after are assigned a pair of likelihoods. The former denotes the likelihood before the changes. The latter denotes the likelihood after the changes. Diagram elements of mode before or after are assigned only a single likelihood. The distinction is likewise for the consequence estimates. Hence, the threat diagrams document not only risks that emerge, disappear or persist, but also how risk levels change. For example, the threat scenario Monitoring of A/C in the sector fails is assigned the likelihood likely before the changes and the likelihood possible after the changes. The likelihood drops due to the introduction of the ADS-B. Information provisioning fails is an unwanted incident, and therefore constitutes a risk. Its likelihood is possible both before and after the changes, while its consequence for the Availability asset is minor as annotated on the relation between the unwanted incident and the asset.

Risk evaluation. During the risk evaluation we first calculate the risk levels by using the risk matrix exemplified in Figure 1 and the likelihood and consequence estimates from the risk estimation. We then compare the risk levels with the risk evaluation criteria to determine which risks that must be treated or evaluated for treatment. The risk estimation is supported by CORAS risk diagrams which we do not show here due to space constraints. These diagrams show the changing risks together with the threats that initiate them and the assets they harm. The unwanted incident Information provisioning fails, for example, has the likelihood possible and the consequence minor before and after the ATM system changes, which yields a low risk level.

Risk treatment. The purpose of the risk treatment is to identify options for risk mitigation for the unacceptable risks. In the presence of changes, the treatments should ensure that an acceptable level of risk is maintained under planned changes or foreseen evolutions. This final step of the process is conducted as a structured brainstorming with a walkthrough of the threat diagrams documenting the unacceptable risks. The CORAS treatment diagrams support such task.

5 Expert Judgement in Evolutionary Risk Analysis

This section discusses further the risk analysis concerned with the Organisation Level Change and the security properties of information protection and information provision. The technical solutions we use in the ATM case study are the modelling language for documenting and reasoning about changing risks, and the assessment method for conducting and documenting the risk analyses of changing and evolving systems. Our work is concerned with supporting structured approaches to changes, capturing security properties affected by changes, and providing mechanisms dealing with subsequent changes. The investigation involved a focused risk analysis of the ATM Changes Requirements and their relevant Security Properties. The risk analysis was conducted by means of design models capturing the main entities characterising an ATM domain. In order to take into account how change requirements, i.e. planned changes that are to be implemented, affect the ATM contexts and their organisations, the risk analysts produced structured (UML) models capturing the ATM settings before and after the changes. These models were reviewed and revised by ATM experts who are currently involved in various activities concerning the SESAR project. The models were used as starting point for the risk analysis in order to have a common understanding of the change requirements among the people (i.e. ATM experts) involved in the risk analysis exercise. Figure 4, for instance, shows a conceptual model of an ACC after changes. The shaded elements represent parts that are introduced to the ACC, whereas the diagonally striped element represents a part that is modified. Similar models have been drawn for other aspects characterising ATM settings and practices (e.g. different UML models capturing different roles and procedures). These models supported discussion and communication between ATM experts and Risk Analysis modellers. Moreover, they have been used to focus and organise the risk analysis on both before and after changes.

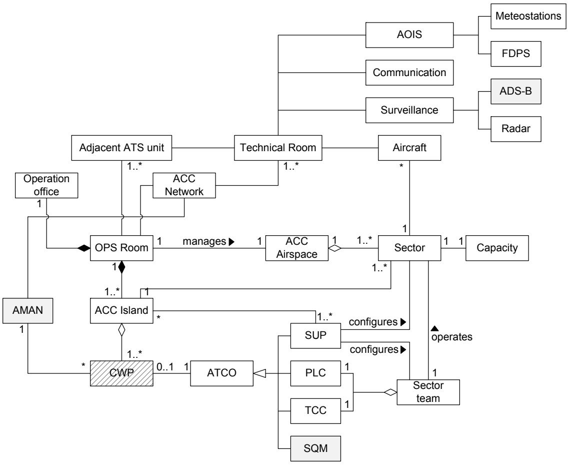


Fig. 4. Conceptual overview of ACC after changes

The risk analysis trial was conducted during a dedicated two-day workshop. The first day of the workshop was dedicated to the risk analysis of the before case. The second day of the workshop was dedicated to the risk analysis of the after case, that is, to the risk analysis regarding the change requirements and how they potentially affect security properties. Table 2 shows examples of the identified hazardous situations modelled and analysed by CORAS diagrams.

Table 2. Examples of hazardous situations

Who/what caused it?	**What is the scenario or incident? What is harmed?**	**What makes it possible?**	**Target element**
System Failure	Loss of the AMAN leads to loss of provisioning of information to ATCO		AMAN
Attacker	Attacker broadcasts false ADS-B signals, which lead to the provisioning of false arrival management data.	Use of ADS-B; dependence on broadcasting	ADS-B
Software failure	Provisioning of unstable or incorrect sequence by the AMAN leading to ATCO reverting to manual sequencing	Immature (unreliable) software	AMAN

The first activity involved a high-level risk analysis of the AMAN introduction. The structured models were used in order to support a walkthrough analysis of the change requirements and to identify potential hazardous situations. The subsequent risk analysis phases involved risk identification, risk estimation and risk evaluation. Figure 5 shows sample risk analysis models for the after case. The model supports a structured risk analysis of change requirements and their impact on critical security properties. Among the risk analysis outcomes were models assessing emergent risk due to the change requirements and their impact on critical security properties. These models supported a systematic way of analysing the risk of changes and their impact on security aspects.

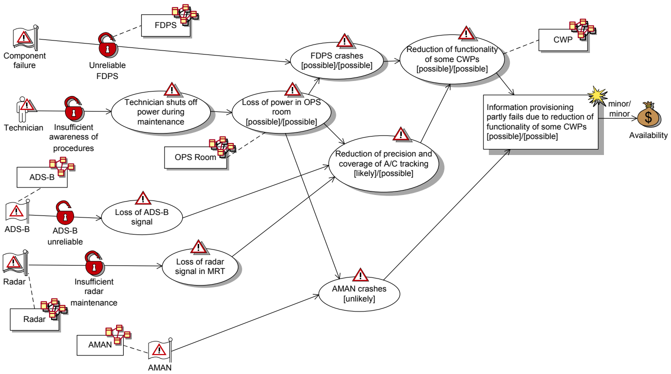

FDPS
Component failure
Unreliable FDPS
FDPS crashes [possible]/[possible]
Reduction of functionality of some CWPs [possible]/[possible]
CWP
Technician
Insufficient awareness of procedures
Technician shuts off power during maintenance
Loss of power in OPS room [possible]/[possible]
OPS Room
Information provisioning partly fails due to reduction of functionality of some CWPs [possible]/[possible]
minor/ minor
Availability
Reduction of precision and coverage of A/C tracking [likely]/[possible]
ADS-B
ADS-B
ADS-B unreliable
Loss of ADS-B signal
Radar
Insufficient radar maintenance
Loss of radar signal in MRT
Radar
AMAN crashes [unlikely]
AMAN
AMAN

Fig. 5. A sample risk model for reduction of functionality

Note that the model captures different hazards and relate them to the target of analysis as well as to other relevant hazards. The resulting network of causalities is used in order to assess the impact of changes on the risk picture and relate them to specific security properties. The same network of causalities is then used to assess the risk in terms of frequency of events and their severities. This is useful to revise risks with respect to emergent hazards related to the change requirements. The final phases involved the identification and discussion of suitable mitigations for the analysed hazards. ATM experts were involved in the risk analysis. They reviewed the models describing the change requirements and actively participated in the risk analysis trial. In order to account for model effectiveness as a means to investigate risk analysis with respect to change requirements, we collected relevant information about the experts' profiles and perceptions. At the beginning of the risk analysis trial, ATM experts as well as other project partners filled in a Safety Culture Questionnaire. The questionnaire has been developed and tailored by Deep Blue taking into account relevant information drawn from the ATM domain [31, 32]. It covered ten different areas (e.g. Regulation and Standards, Safety Assessment) by fifty three questions contributing to Safety Culture. Figure 6 shows a Safety Culture Profile for one of the ATM experts taking parts in the risk analysis trials.

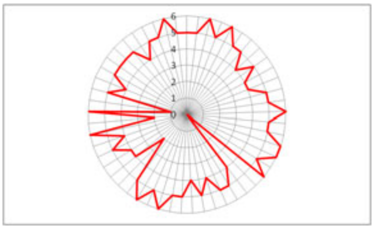
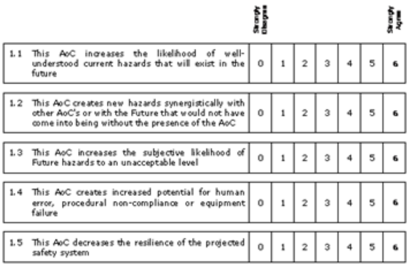


Fig. 6. Safety Culture Profile

The reason we collected expert knowledge with respect to Safety Culture is because Risk Management and Change Management are often critical practices. This allows us to understand further the relationship between safety and risk with respect to change requirements and relevant security properties. After each one of two risk analysis sessions, we collected other information by an Evolutionary Risk Questionnaire. Figure 7 shows some of the questionnaire statements.



		Strongly Disagree						Strongly Agree
1.1	This AoC increases the likelihood of well-understood current hazards that will exist in the future	0	1	2	3	4	5	6
1.2	This AoC creates new hazards synergistically with other AoC's or with the Future that would not have come into being without the presence of the AoC	0	1	2	3	4	5	6
1.3	This AoC increases the subjective likelihood of Future hazards to an unacceptable level	0	1	2	3	4	5	6
1.4	This AoC creates increased potential for human error, procedural non-compliance or equipment failure	0	1	2	3	4	5	6
1.5	This AoC decreases the resilience of the projected safety system	0	1	2	3	4	5	6

Fig. 7. Sample questionnaire statements

The questionnaire has been developed and tailored by Deep Blue in order to account of perceived hazards, hence risk perception, as captured by risk analysis models concerning current and future change requirements. The questionnaire consists of twelve different points drawn from relevant work in the ATM domain [33], and is concerned with Area of Changes (AoC) as a means to discuss relevant changes requirements and hazards pertinent to current and future ATM. Figure 8 shows the questionnaires' outcomes (for the same expert). It is interesting to notice how risk perceptions change with respect to current situation and future ones. The dedicated risk analysis sessions helped to capture this shift in perception with respect to change requirements. The specific points highlighted by the questionnaire identify aspects for further investigation in order to refine and gain confidence on the risk analysis concerning future changes requirements.

The identification of specific areas of concerns for changes supports the use of structured models in order to assess the impact of changes. However, evolutionary risk analysis needs to be organised and supported adequately.

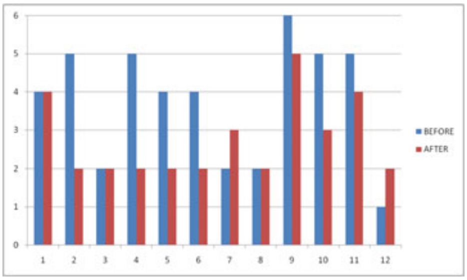


Fig. 8. Evolutionary risk perception

6 Conclusions

This paper enhances how structured models may support expert judgement while conducting an evolutionary risk analysis. The use of structured models tailored and organised for an evolutionary risk analysis helps to identify potential areas of concerns due to changes. The evolutionary risk analysis presented in this paper consists of different activities: (1) identify relevant design models, (2) build risk assessment models for before and after the changes, (3) run dedicated before and after risk analysis sessions, (4) monitor (by means of qualitative assessment) risk perception shifts in order to identify areas of concerns. Our empirical results provide insights supporting evolutionary risk analysis by means of structured models and expert judgement. The generality of the different activities would support the evolutionary risk analysis across different domains. Further work intends to involve an increasing number of experts in order to gain further evidence supporting evolutionary risk analysis, but also to support statistical accounts of how changes affect risk perceptions in risk analysis.

Acknowledgements. This work has been supported by the *Security engineering for lifelong evolvable systems* (SecureChange) project, FP7-EC-GA-231101.

References

1. ISO 31000, Risk Management: Principles and Guidelines, International Organization for Standardization (2009)
2. Alberts, C.J., Davey, J.: OCTAVE criteria version 2.0. Technical report CMU/SEI-2001-TR-016. Carnegie Mellon University (2004)
3. Barber, B., Davey, J.: The use of the CCTA risk analysis and management methodology CRAMM in health information systems. In: 7th International Congress on Medical Informatics, MEDINFO 1992, pp. 1589–1593 (1992)
4. CRAMM - The total information security toolkit, `http://www.cramm.com/` (accessed March 2, 2011)
5. Robinson, R.M., Anderson, K., Browning, B., Francis, G., Kanga, M., Millen, T., Milman, C.: Risk and Reliability. An Introductory Text, 5th edn. R2A (2001)
6. IEC 61025, Fault Tree Analysis (FTA), International Electrotechnical Commission (1990)

7. IEC 60300-3-9, Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems - Event Tree Analysis (ETA), International Electrotechnical Commission (1995)
8. Schneier, B.: Attack trees: Modeling security threats. Dr. Dobb's J. 24(12), 21–29 (1999)
9. Nielsen, D.S.: The cause/consequence diagram method as basis for quantitative accident analysis. Technical report RISO-M-1374, Danish Atomic Energy Commission (1971)
10. Ben-Gal, I.: Bayesian networks. In: Ruggeri, F., Kenett, R.S., Faltin, F.W. (eds.) Encyclopedia of Statistics in Quality and Reliability. John Wiley & Sons, Chichester (2007)
11. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer, Heidelberg (2011)
12. Brændeland, G., Refsdal, A., Stølen, K.: Modular analysis and modelling of risk scenarios with dependencies. Journal of Systems and Software 83(10), 1995–2013 (2010)
13. Lund, M.S., Solhaug, B., Stølen, K., Innerhofer-Oberperfler, F., Felici, M., Meduri, V., Tedeschi, A.: Assessment Method, SecureChange deliverable (2011)
14. OMG Unified Modeling Language, Superstructure, version 2.2, Object Management Group (2009)
15. Perrow, C.: Normal accidents: living with high-risk technologies. Princeton University Press, Princeton (1999)
16. Edwards, E.: Man and machine: Systems for safety. In: Proceedings of British Airline Pilots Associations Technical Symposium, British Airline Pilots Associations, pp. 21-36 (1972)
17. Reason, J.: Managing the Risks of Organizational Accidents, Ashgate (1997)
18. Pasquini, A., Pozzi, S.: Evaluation of air traffic management procedures - safety assessment in an experimental environment. Reliability Engineering & System Safety 89(1), 105–117 (2005)
19. Pasquini, A., Pozzi, S., Save, L.: A critical view of severity classification in risk assessment methods. Reliability Engineering & System Safety 96(1), 53–63 (2011)
20. EUROCONTROL. Safety Nets - Ensuring Effectiveness (2009)
21. EUROCONTROL safety regulatory requirements (ESARR), ESARR 4 - risk assessment and mitigation in ATM, Edition 1.0 (2001)
22. EUROCONTROL safety regulatory requirements (ESARR), ESARR 6 - Software in ATM Systems, Edition 1.0 (2003)
23. EUROCONTROL, Baseline Integrated Risk Picture for Air Traffic Management in Europe, EEC Note No. 15/05 (2005)
24. Brooker, P.: The Überlingen accident: Macro-level safety lessons. Safety Science 46(10), 1483–1508 (2008)
25. Felici, M.: Evolutionary safety analysis: Motivations from the air traffic management domain. In: Winther, R., Gran, B.A., Dahll, G. (eds.) SAFECOMP 2005. LNCS, vol. 3688, pp. 208–221. Springer, Heidelberg (2005)