ARIEL • Air Traffic Resilience

Recommendations to Strengthen the Cyber-Resilience of the Air Traffic System

Version 2.0 – 31 July 2017

IABG
DFS Deutsche Flugsicherung
Universität der Bundeswehr München
Hochschule für angewandte Wissenschaften München
AIRBUS
Bauhaus Luftfahrt Neue Wege.
Fraunhofer AISEC
DLR

– This page intentionally left blank –

LUDWIG BÖLKOW CAMPUS
AEROSPACE | SECURITY

Supported by the
Free State of Bavaria

Recommendations to Strengthen the Cyber Resilience of the Air Traffic System

Editors:

T. Kiesling	IABG Einsteinstr. 20, 85521 Ottobrunn kiesling@iabg.de
M. Kreuzer	University of Applied Sciences Munich Lothstr. 64, 80335 München marcus.kreuzer@hm.edu

Contributors:

T. Kiesling, J. Ziegler, T. Rieth	IABG
D. Schupke, A. Exposito-Garcia	Airbus Group
S. Biermann-Höller, M. Krempel	DFS
D. Schuster	Fraunhofer AISEC
G. Dreo Rodosek, O. Rose T. Bierwirth, T. Mayer	Universität der Bundeswehr München
C. Jeßberger	Bauhaus Luftfahrt
A. Knoll, M. Kreuzer	University of Applied Sciences Munich
M. Schnell, O. Osechas, A. Schmitt, C. Edinger	DLR

– This page intentionally left blank –

EXECUTIVE SUMMARY

As part of the overall transport infrastructure, air transportation is defined as a critical infrastructure. Recent approaches to increase capacity and efficiency of the existing air traffic system like Single European Sky in Europe or NextGen in the U.S. lead to an enormous effort of transition towards digitalization and automation. In this process, formerly separated IT systems get connected via newly established networks for information and data exchange. Due to a growth of complexity, the attack surface of the overall system is increasing and previously unknown interdependencies are being created. Limiting security risk management to "traditional" physical aspects like air terrorism is no longer sufficient to ensure a stable and robust operation of the air transportation system. A component of cyber resilience has to be added to traditional risk mitigation approaches.

The ultimate aim of the Air Traffic Resilience (ARIEL) project is to strengthen the overall air traffic system resilience against cyber threats. To achieve this, the project focusses on the development and evaluation of holistic approaches for cyber risk analysis and assessment. To permanently provide a high level of resilience, ARIEL proposes to introduce a continuous dynamic and model-based cyber risk analysis process. To establish persisting capabilities of cyber resilience in the air transportation system, we identified seven building blocks, which we understand as essential for implementation:

1) Develop the structural and procedural basis for continuous intra- and inter-organizational cyber resilience analysis: We recommend combining classical information security and newly developed cyber operational resilience approaches by establishing an organizational structure that brings together the personnel of all relevant disciplines inside and across air traffic organizations to cope with the evolving cyber threat landscape in a holistic way. This has to be combined with suitable continuous processes aligned with the existing information security norms and standards.

2) Develop and manage interdisciplinary cyber risk analysis teams: To facilitate the establishment of interdisciplinary collaborating teams, we recommend to develop and apply the necessary methods and management approaches comprising elements of a common language; knowledge management and transfer; ignorance management for balanced evaluation of findings; widespread basic IT knowledge and security awareness by personnel of all disciplines including middle and top management.

3) Develop and maintain a portfolio of cyber threat scenarios: In contrast to the currently applied ad hoc way of threat scenario development and utilization, we recommend the introduction of a structured continuous process for the development and evolution of air-traffic cyber threat scenarios. This is to be combined with suitable methodology to develop scenarios and to apply them in the areas of knowledge development, training as well as verification and validation. To increase the potential for reuse and sharing of scenarios standardized scenario representation formats and data interfaces need to be developed.

4) Ensure the interoperability of cyber-relevant models and data: We recommend developing standardized meta-models for computer-based data exchange, collaboration of different models and the integration and comparison of cyber-relevant results and findings in tool-based analysis and decision support. To enable interdisciplinary or even inter-domain collaboration based on a comprehensive approach, data sharing concepts are needed for a reuse of existing data, which include technical, methodological and organisational aspects.

5) Refine and Evolve Dynamic Risk Analysis Methods: We recommend putting additional effort into the further evaluation and evolvement of the model-based dynamic risk analysis method developed in

the ARIEL project. This semi-automated analysis method enables us to dynamically model and analyze cyber risks in complex systems, large organizations or even in between several interconnected organizations. We believe in the high potential of this approach to enable a comprehensive, dynamic cyber risk assessment in the aviation sector. Currently, we envisage its application in the areas of secure systems engineering, information security operations, security governance and oversight as well as its transferability to other domains.

6) Safety & Security – Ensure consistency and enable synergies: Since cyber threats and potential cyber-attacks can have a direct impact on safety-critical system functions, we recommend developing a comprehensive risk management approach aligning the formerly separated considerations of safety and security under a common roof. For this purpose, we found some new criteria, which have to be added to development processes to apply findings and results of comprehensive risk assessments in a suitable way to the air traffic system.

7) Enhance design methodologies to ensure resilient system characteristics throughout a complete lifecycle: We recommend restructuring the architectures of socio-technical systems (specifically the air traffic system) to support cyber resilience in addition to protective measures. Existing approaches of resilience engineering, which focus mainly on human factors in complex systems, have to be extended in a technical sense towards integration of cyber resilience capabilities. Some of the more important aspects to be considered are: the preparation of architectures for ongoing changes; the consideration of mitigation and recovery strategies in the system design; and the addition of system functions supporting the detection of cyber-attacks.

8) Exploit simulation methodologies to support cyber threat and risk analysis of complex systems: To achieve a holistic understanding of the effects of potential cyber-attacks in complex systems, simulation is a valuable method to complement more traditional analysis methods. We recommend a more widespread application of simulation models for processes and systems identified by cyber threat and risk analysis to be critical for system operation. Simulation increases the understanding of the impact of identified cyber threats and supports the validation of risk analysis results. Besides using existing simulation models as standalone tools, we recommend to connect and develop simulation models “from gate-to-gate” to support holistic analysis of aviation processes. Finally, we also recommend using human-in-the-loop simulation with operational staff to research the fundamentals of human factors in the face of potential cyber-attacks.

These recommendations result from the experiences made while applying a holistic approach of cyber risk analysis to the air transportation sector. This application revealed some issues, which have to be resolved on the basis of further development and implementation of the above-mentioned aspects. When properly followed up by further research, these results and findings will help to strengthen the resilience of the air traffic system against cyberattacks. Furthermore, they also demonstrate a potential way forward in other domains in the field of critical infrastructures.

TABLE OF CONTENTS

– This page intentionally left blank –

1 INTRODUCTION

According to EU and German legislation, air transportation is a critical infrastructure[1]. Its importance to the overall European transportation sector was impressively demonstrated by a relatively small eruption of a volcano on Iceland in 2010. As a single, regional event it produced an ash cloud which covered parts of northern Europe for six days and grounded about 100.000 flights. The incident affected 10 million passengers and the economic damage to airlines was estimated between 1.5-2.5 billion Euros. The impact of this unforeseen disruption revealed the sensitivity of this highly efficient system, which was seen as being unquestionably robust and reliable by the public until then.

Air transportation has a long history of risk management with a special focus on safety and physical security. In the last two decades, the field of cyber risks have come into existence. Accompanied by the SESAR-JU, the European Commission undertakes ambitious efforts to increase performance of the overall air transport system within the programme Single European Sky (SES) to adapt aviation in Europe to the global ambitions laid down in the Global Air Navigation Plan (GANP[2]) by the International Civil Aviation Organization (ICAO). The performance ambitions are supported by an ongoing, cost- and optimization-driven development for digitalisation and automation of systems and processes. This leads to a constant raise of interconnections and interdependencies of constituents of the aviation system. The interfaces, increasingly built on standardized hardware units and software modules, connect specific attack surfaces of formerly separated system areas and therefore add a new dimension of cyber-related risks to the overall air traffic system. Through cascading effects and correlations, single cyber-attacks may have the potential to induce a system-wide impact on the air transportation sector, which could cause a collapse-like disruption of scheduled air traffic management (comparable to the above-mentioned incident). Known attacks give a first impression of the vulnerability of the overall system, e.g. at the Warsaw airport against the Polish airline LOT in 2015[3].

To reduce the vulnerability to cyber-related risks, it is the overall aim of the ARIEL project to strengthen the air transportation systems resilience against cyber threats, which is seen as the capability of an organisational and technical system to protect itself from failures or losses, to mitigate impacts by adaption to changing conditions and to recover from degradation after the incident. A holistic, interdisciplinary approach is applied to pursue a comprehensive, continuous risk analysis of potential cyber-attacks, based on scenario methods to cope with the growing complexity of the air traffic system. To go a step further, ARIEL applied a prototype of a tool based decision support within cyber security risk assessment. Our approach combines an attack model, a model of the target of attack and an impact model to enable a computer based reasoning and analysis for a dynamic risk analysis. Based on continuously derived risk indicators, measures can be taken to manage weaknesses and to reinforce resilience.

As a result of our work within the ARIEL project, we identified eight areas of potential improvement, which we believe to be essential for a successful constitution of cyber resilience in this domain. They are presented in Chapter 2.

[1] Directive (EU) 2016/1148 Articles 4 and 5; Germany: IT-Sicherheitsgesetz Artikel 1.
[2] http://www.icao.int/publications/Documents/9750_4ed_en.pdf.
[3] http://uk.reuters.com/article/uk-poland-lot-cybercrime-idUKKBN0P10WY20150621 (visited 8.12.2016).

2 RECOMMENDATIONS

This chapter deals with the eight building blocks of central recommendations. Each building block will be explained in detail in a sub-chapter. Chapter 2.1 gives an overview of the current standards and developments regarding cyber security and cyber resilience, focusing on risk analysis approaches and their integration into business processes. It connects the other chapters thematically and therefore embraces their contents.

Chapter 2.2 discusses the comprehensive approach of the ARIEL project in regards to the constitution of collaborating, interdisciplinary teams. The creation of interdisciplinary teams lays the foundation of a balanced and comprehensive risk analysis. Based on scenario methods and the input of the different team members, a comprehensive model of the observed overall system has to be created to reduce complexity. Aspects for further development of scenario based methods and additional possibilities for the application of those methods are presented in Chapter 2.3. Since the exchange and presentation of findings, knowledge and data are crucial for efficient, interdisciplinary collaboration within risk analysis, common data formats and standardized interfaces are needed. Therefore, we see data management as a fundamental basis for the interaction of all steps of a risk analysis and further development of cyber resilience in socio-technical systems. See Chapter 2.4 for our conclusions. A prerequisite for efficient dynamic risk analysis (Chapter 2.5) is the scenario-based approach introduced in Chapter 2.3. Standardized data and information, like proposed in Chapter 2.4, is mandatory for efficient risk analysis. Chapter 2.8 contains further recommendations with respect to the application of simulation methodologies for cyber resilience threat and risk analysis. It is the result of a second phase of the ARIEL project executed after the initial version of ARIEL recommendations was created. Thus, Chapter 2.8 is new in Version 2.0 of this document.

Chapters 2.6 and 2.7 frame the other chapters' emphasis on providing an operational view on socio-technical systems: Chapter 2.6 addresses the common approach to safety and security assessments considering all hazards with their potential impact on the different performance aspects of aviation, notably in terms of capacity, efficiency and the protection of life and limb. Chapter 2.7 describes possibilities, how to enable the overall system to accept the restructuration from a technically protected, safety and security orientated shape of the system to the implementation of a holistic approach of resilience, based on results and findings of risk analysis.

<table>
<tr>
<td rowspan="3">Chapter 2.7:
Enhance design methodologies to ensure resilient system characteristics throughout a complete lifecycle</td>
<td colspan="4">Chapter 2.1:
Develop the structural and procedural basis for continuous intra- and inter-organizational cyber resilience analysis</td>
<td rowspan="3">Chapter 2.6:
Safety & Security: Ensure consistency and enable synergies</td>
</tr>
<tr>
<td>Chapter 2.2:
Build and manage interdisciplinary cyber risk analysis teams (organizational / personnel)</td>
<td>Chapter 2.3:
Develop and maintain a portfolio of cyber threat scenarios (methodological)</td>
<td>Chapter 2.5:
Refine and Evolve Dynamic Risk Analysis Methods</td>
<td>Chapter 2.8:
Exploit simulation methodologies to support cyber threat and risk analysis of complex systems</td>
</tr>
<tr>
<td colspan="4">Chapter 2.4:
Ensure interoperability of cyber-relevant models and data</td>
</tr>
</table>

Figure 1: Structure of the document.

2.1 DEVELOP THE STRUCTURAL AND PROCEDURAL BASIS FOR CONTINUOUS INTRA- AND INTER-ORGANIZATIONAL CYBER RESILIENCE ANALYSIS

There are many standards and best practices describing the implementation, operation and maintenance of an Information Security Management System (ISMS) within an organization, which amongst others defines procedures and responsibilities to improve the level of cyber security in the organization. One of the main ideas in all these norms is continuous improvement with risk analysis playing an important role – at least in theory.

The ISO 27000-series[4] describes the design of an ISMS with the PDCA-Cycle (Plan-Do-Check-Act). Best practices like ITIL[5] and COBIT[6] specify certain goals and do the service design, transition and operation within a life cycle. To improve the level of cyber security steadily, it is crucial to perform information security risk analysis on a regular basis. Repetitive risk analysis is needed to adapt to changes inside a system as well as to its environment notably in terms of threats and vulnerabilities. This requires the definition of key performance indicators, which are intended to judge the security programs' improvement. Besides those operational and technical basic principles, it is also essential to setup a clear and consistent information security governance structure. That means, that the top management of an organization has to derive the security strategy from business objectives in a top-down approach and empower its subordinates, like the CIO or CISO, to enforce the planned measures.

In practice, the implementation of a measurable, continuously improving security program is a major challenge that is very hard to solve. There are several reasons to this, not the least of which is the still lacking awareness of management about the importance of cyber security and the resulting lack of determination to drive cyber security improvement. Methodical and organizational approaches, like the OCTAVE model developed by the SEI-CERT[7], could be of help to solve these issues, but are rarely applied. The basic idea of this approach is the continuous (i.e. periodical) conduction of the risk analysis tasks of an organization by a fixed team of personnel that is recruited from the various parts of the organization.

Other newer approaches such as the CERT Resilience Management Model of the Carnegie Mellon University[8] and the U.S. Electricity Subsector Cybersecurity Capability Maturity Model[9] illustrate procedures to identify and assess the maturity of cyber resilience of an organization on the level of business objectives and business processes. This is a new approach to cybersecurity capability modeling, as it aims to integrate IT operations and business continuity processes with security management processes. Furthermore, the models measure the maturity related to the implementation of these processes. This indicates the direction, which has to be taken by a more holistic approach to cyber security, moving from a purely information-security-centric approach towards comprehensive resilience management processes.

[4] International Standards Organisation – ISO (2016); ISO27000:2016(en) - Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[5] Axelos (2011). IT Infrastructure Library, Version 3.
[6] Information Systems Audit and Control Association – ISACA (2012). COBIT 5.0.
[7] Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE Approach. Pittsburgh, PA, Carnegie Mellon University.
[8] Butkovic, M. J., Caralli, R. A. (2013). Advancing Cybersecurity Capability Measurement Using the CERT ® -RMM Maturity Indicator Level Scale. Pittsburgh, PA, Carnegie Mellon University.
[9] US Department of Energy (2014). Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1.

In practice, cyber resilience analyses are typically not performed regularly. The corresponding organizational foundations are still a matter of research. For instance, the Cybersecurity Strategic Research Agenda, which has been developed recently by the European Network and Information Security Platform sponsored by the European Commission[10], emphasizes the need to improve cyber security risk and resilience management and analysis approaches, both in the methodological and organizational dimension, as well as to improve tool support. Another example is the Roadmap to Secure Control Systems in the Transportation Sector, which has been developed in 2012 by a working group sponsored by the U.S. Department of Homeland Security[11]. This document considers the implementation of continuous risk and resilience management processes in the transportation sector as a long-term goal with a time horizon of about ten years.

Typical approaches to risk analysis focus on the more or less isolated analysis of cyber risks connected with a single component of the overall system. The ambition of a holistic approach is to analyze cyber risks on a system (or even system-of-systems) level and to integrate all necessary views in the process. Of special importance is the operational view of a system, which is focused on the business processes that constitute a service (e.g. the air traffic management processes connected with the operation of flights in Europe). When examining the potential impact of cyber threats on an operational level, the focus of risk analysis shifts from classical information security towards cyber operational resilience.

"When examining the potential impact of cyber threats on an operational level, the focus of risk analysis shifts from classical information security towards cyber operational resilience."

Especially in the field of air transport, where the degree of complexity is rising with the steady increase of embedded IT systems, it becomes more important to establish an organizational structure and processes which is able to cope with the transdisciplinary and coordinative nature of this security problem. The holistic, resilience-oriented view taken in the ARIEL project strongly confirmed this issue and led to the identification of several aspects relevant for solving this challenge. Note, that this result of the ARIEL project is not unique and original in nature, but rather is relevant due to the confirmation that we can give with respect to the importance of developing the structural and procedural basis for continuous intra- and inter-organizational cyber resilience analysis. Furthermore, this recommendation serves to link various other ARIEL recommendations to each other.

Finally, we recommend developing the structural and procedural basis for continuous intra- and inter-organizational cyber resilience analysis in the air traffic system at large. The core aspects of this issue are discussed in the following.

Recommendation

Combine protection and resilience views for a holistic approach.

We propose to shift the view of cyber security programs from the currently dominant largely protective approaches to balanced holistic approaches combining protective and resilience measures. Specifically, in the air transport sector, more emphasis has to be given to cyber operational resilience as a view, integrating business continuity and disaster recovery approaches. A first step in this direction could be the adaption of resilience-oriented process models[12] in air transport organizations.

[10] Bisson, P., Martinelli, F., Riesco Granadino, R. (2015). Cybersecurity Strategic Research Agenda – Produced by the European Network and Informations Security Platform.
[11] US Department of Homeland Security (2012). Roadmap to Secure Control Systems in the Transportation Sector.
[12] For instance, the CERT resilience management model of the SEI-CERT of the Carnegie Mellon University in Pittsburgh.

Organize teams on Intra- and inter-organizational level.

A comprehensive understanding of cyber threats and risks on the level of business objectives and processes necessitates the collaboration of all relevant stakeholders inside and across interconnected entities in the air traffic system. In order to follow a holistic approach as discussed above, all relevant views must be considered. The involvement of stakeholders from all relevant parts of the organization is needed in order to create a team which is responsible for delivering the risk analysis process as part of continuous risk management in the organization. This is the *intra*-organizational dimension of collaboration. The other dimension is the *inter*-organizational one, where the collaboration between the various entities of the air traffic system is a key aspect to comprehensively approach the security problem. The latter aspect has been emphasized extensively by many experts in the past, but is still an open issue that has to be solved in the air traffic system. With respect to the above-mentioned approach of setting up virtual risk analysis teams of organizations, the interfaces for inter-organizational collaboration have to be considered, as well.

Perform resilience management as a continuous process.

The continuous nature of resilience management as well as the continuous evolution of the protected system is necessary due to an ever-changing threat environment. Although the periodic execution of a risk analysis phase of a security program is a good start, the approach should be driven further to a truly continuous approach. We envision an event-driven mode of operation, where an organization must be enabled to react to events with respect to the threat environment as well as to change own infrastructures and systems. Note, that this necessitates the availability of powerful and easy-to-use risk analysis tools. The ARIEL dynamic risk management methodology and tool is aimed to support this approach, see Chapter 2.5.

Ensure a long-term stable nature of risk and threat analysis teams.

It is essential to follow a long-term strategy in the establishment of risk and threat analysis teams as a prerequisite for efficient team operation. This means that team membership should be as stable as possible. Processes need to be established to be able to regenerate in cases of membership change and to evolve with changing environments. Drastic changes in membership should be avoided as far as possible. Team membership changes should rather be evolutionary. We conclude that suitable methods and tools are needed to support this continuity. From our point of view, scenario-orientation and ontology management are central aspects to enable interdisciplinary understanding. On the one hand, scenarios as specific examples help to achieve mutual understanding more easily and efficiently. On the other hand, a common language is a key aspect to common understanding. Thus, both parts need to be actively managed. Chapter 2.2 shows how to develop and manage interdisciplinary teams, whereas Chapter 2.3 presents thoughts about a scenario-based approach.

Support consistency and stability through regulation.

The motivation to implement the continuous approaches of this recommendation can be intrinsic or extrinsic. The intrinsic motivation has to be derived from the business objectives of organizations. This is largely the task of the top management. The major route to achieve this is by raising awareness. However, this should be supported by effective regulations as well as strict enforcement of these regulations. With respect to the specific focus of this recommendation, organizational items like architectures and processes need to be considered for regulation (e.g., direct reporting of information security management to top management/CEO, detailed specifications of continuous risk analysis/management processes in standards and directives).

2.2 DEVELOP AND MANAGE INTERDISCIPLINARY CYBER RISK ANALYSIS TEAMS

Cyber security and, thus, cyber risk analysis is an important task to improve, maintain or – ideally – ensure cyber resilience. Due to the interconnectedness of the participants within the aviation system, this task should be taken seriously by each company in order not to be the starting point of a cyber-attack with contagion effects, which harm many or even all other players in the aviation system. As cyber security affects, as well as is affected, by each individual employee, a company and the aviation system all disciplines in this system can – and should – play an active role to improve, maintain and ensure cyber resilience in order to maintain performance of their respective tasks and goals. Thus, managing interdisciplinary cyber risk analysis teams is a key recommendation which had been derived from the ARIEL research project. This could be achieved by the following sub-tasks or partial recommendations:

Recommendation

Support industrial democratization of interdisciplinary collaboration

Cyber Security originates in the IT and is often seen to be handled by IT experts. Even though the management has the responsibility for the arrangement of cyber security in his company (see e.g. requirements of an information security management system (ISMS) in ISO 27001[13]), they often see the IT department to be the only institution to take care for cyber security[14]. As cyber security has an impact on all assets of a company, it is advisable to put confidence in a Chief Information Security Officer (CISO), who can pool the diverse requirements of cyber security for the company. Another new idea in the media is to install a Chief Digitalization Officer (CDO) as part of top management with direct reporting to the CEO. This would shift the view of cyber security towards integrating it in the risk view of digitalization and could be another good way forward with respect to cyber security management.

For a comprehensive view on cyber security and internal or external threats the specific information on internal or external processes should be taken into account as well as data exchange from employees of different disciplines, in different positions in a company and of other stakeholders. The evaluation of the specific information needs to be equally balanced between all disciplines to avoid having only one way of looking on things. Thus, each discipline needs to enjoy equal rights in an interdisciplinary team. In other words, a democratization of the organization of such a team is important to enable a fruitful collaboration for cyber risk analyses.

Manage ignorance with respect to the user or the problem

Ignorance is a state or fact of being unaware of issues, because these issues are neglected or not wanted to be known. Further, ignorance can occur in consequence of a selection process due to scarcity in time or resources. Especially in interdisciplinary teams, but also due to group dynamics, misunderstanding can lead to ignoring issues (similar to ideas of securing the diversity of opinions regarding minority groups), even though they are objectively target-aimed and could represent a game changer. This effect can be intensified if there are a predominant number of people from one professional discipline. For example, an engineer can develop solutions to many technical problems including an evaluation of the goodness of this solution. With this solution in hand the probability to sort out or ignore any other solution is high and can be even higher if engineers outnumber all other members in an interdisciplinary team. Please be aware that the same is true for all professional disciplines that constitute the majority in an interdisciplinary team. Additionally, as this is a classical human phenomenon,

[13] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization, 2013. URL: http://www.iso27001security.com/html/27001.html.

[14] „Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen“, Bundesamt für Sicherheit in der Informationstechnik, 2011. URL: https://www.internet-sicherheit.de/fileadmin/docs/downloads/andere_studien_dokumente/BSI/2011_Studie-IT-Sicherheit-KMU.pdf.

basic approaches need to be developed to form interdisciplinary teams which can bear at least partial ignorance.

Further, in order to avoid or to reduce the probability of ignoring objectively target-aimed issues, an appropriate ignorance management should be applied. Such an ignorance management could use features from democratic political instruments like political opposition or minority rights.

Transfer knowledge and raise awareness of cyber security

Knowledge transfer and raising awareness of potential risks is a matter of common knowledge in many fields. But in the context of aviation cyber security this also means to think outside of the box and transfer knowledge across different disciplines as the aviation system is heavily interconnected, such that contagion effects matter as much as individual corporate risks of cyber-attacks. Because of the interdisciplinary approach within ARIEL, all partners – whether with profound cyber security knowledge or not – have facilitated the knowledge transfer and, thus, the raise of awareness of cyber resilience issues.

"…think out of the box and transfer knowledge across different disciplines as the aviation system is heavily interconnected, such that contagion effects matter as much as individual corporate risks of cyber-attacks"

Activities to raise awareness of cyber security should be prioritized at all aviation stakeholders. These activities should lay a special emphasis on non-technical aspect of cyber security with very limited technical solutions, like "social engineering", which means manipulating or using humans to get unauthorized access to IT systems. With the aid of a knowledge management system (e.g. within LBC), the gathered cyber security knowledge should be edited and stored to be easily retrieved. This is especially important, because the transferred knowledge about cyber security can quickly get lost due to project consortia change or job change of individuals. Some facts and potential solutions to ease data exchange on machine level are shown in Chapter 2.4.

Develop collaboration and communication

Collaboration and communication heavily depend on a uniform terminology. Each team member has a different perspective of the same aviation system, which may lead to a lack of coherent perception of the aviation system's reality, which is applicable to every problem solution. Moreover, a key challenge is to find and define a common forum to develop a problem specific model of the aviation system, in which all participants are able and are willing to share their insights. Collaboration already exists e.g. for companies and sectors with regard to critical infrastructure, i.e. UP KRITIS in Germany[15] and critical infrastructure protection at the European level[16]. While security-related collaboration within the aviation sector exists for a long time in physical security, cyber security still shows a low level of collaboration with some initial global and regional activities of stakeholder organizations like CANSO, ACI and IATA and, respectively, in Germany with BDL's[17] cyber security working group. Aviation crisis management, i.e. EUROCONTROL's crisis management organization, emerges as a facilitator

[15] http://www.kritis.bund.de.
[16] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l33259.
[17] https://www.bdl.aero.

Recommendation

through the extension of its scope to cyber crisis scenarios[18]. Collaboration between industry and research includes the Ludwig Bölkow Campus[19], SESAR[20] and other European or national research projects. ARIEL is a good example of working collaboration and communication between researchers from different disciplines and industrial partners, as there are IT and cyber security experts, analysts, safety and security experts, economists, mathematicians, pilots and aeronautical engineers.

An overall goal should be to find and define a common forum to develop a problem specific model of the aviation system, in which all participants are able and are willing to share their insights, like the architectural representations of the subject area like the European ATM Architecture (EATMA) and in the ICAO Global Air navigation Plan (GANP). The usability and reusability of research findings for industrial purposes as well as for further research projects should be given much more priority.

Integrate stakeholders and manage contradictions and layers of security

In line with the above-mentioned stakeholder organizations, integrating stakeholders and managing contradictions and layers of security is an issue. The stakeholder dialogue, or better the integration of many stakeholders in one project – like in ARIEL – is an effective approach of enabling interdisciplinary and cross-disciplinary communication and collaboration. Together, contradictions, layers of security and its different (and often divergent) perspectives can be managed much more targeted, than only speaking about one another. To that end, ARIEL also makes use of the holistic and integrative approach that drove the development of the EATMA.

The stakeholder dialogue or better the integration of many stakeholders in one project should be facilitated within future projects, as it is an effective way of enabling interdisciplinary and cross-disciplinary communication and collaboration. A way to support the communication process is the application of scenarios (see Chapter 2.3).

Distribute basic knowledge in IT and cyber security

Effective application of cyber security in systems like aviation builds on knowledge that is transversal across different application sectors. The general improvement of basic IT and cyber security knowledge will be instrumental across all areas of private and professional life in order to raise awareness of cyber risks and to build at least basic knowledge to avoid or prevent those risks. In aviation, cyber incidents are currently seen as quite rare. As consequence, topics in cyber security are currently only secondary. This needs to be changed and adopted since cyber security risks can potentially have immense negative impacts e.g. on corporate level, human life and limb as well as on aviation key performance areas.

Beginning at schools and at universities, but also during advanced education activities, topics in IT and cyber security should be taught across all areas. Exercises, simulations and serious gaming are good alternatives to go viral while imparting knowledge to decision makers and relevant operative staff. This applies for aviation specific key performance areas as well as all other areas using digital data.

To sum up, there are two major lines of development which aim at developing and managing interdisciplinary cyber risk analysis teams:

[18] http://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc.
[19] http://www.lb-campus.com.
[20] http://www.sesarju.eu/.

On the one hand, barriers need to be cleared, which hinder the formation as well as the performance of a working cyber risk analysis team, i.e. to support industrial democratization of interdisciplinary collaboration and to manage ignorance with respect to the user or the problem.

On the other hand, enablers and facilitators need to be part of the interdisciplinary cyber risk analysis teams. For that purpose, it is important to conduct a systemic analysis which supports the assessment of side and long-term effects and the revelation of risks. This analysis aims at transferring knowledge and raising awareness of cyber security, at developing collaboration and communication, at integrating stakeholders and managing contradictions and layers of security as well as at distributing basic knowledge in IT and cyber security.

2.3 DEVELOP AND MAINTAIN A PORTFOLIO OF CYBER THREAT SCENARIOS

Cyber security comprises a wide range of elements which need to be considered to effectively and continuously enforce cyber resilience and prevent cyber-attacks (cf. e.g. ECB 2016[21]). A major task in order to oversee these manifold tasks, people and disciplines to be involved is to divide them in readily understandable but knowledgeable and transparent scenarios. Thus, a key role in cyber security is to develop and maintain a portfolio of cyber threat scenarios.

Recommendation

Develop scenarios for training purposes

Considering the above mentioned key role of scenarios to oversee tasks, people and disciplines involved in or affected by potential cyber threats, special emphasis should be placed on developing scenarios for training purposes (e.g. of emergency situations). Many different scenarios have been developed in the context of aviation safety and security as a part of risk assessments and for exercise and training purposes. Examples include EACCC exercises at EUROCONTROL, Pandemic-LÜKEX 2011 aviation scenarios, Cyber-LÜKEX 2011, the civil-military exercise during MNE7 as well as scenarios regarding security risk analyses within SESAR[22]. Decisions on the severity of incidents have been made by humans in all these trainings.

Scenarios are an important basis to simulate and, thus, to train emergency situations. Besides the (further) development of scenarios, realistic simulations are a key enabler for efficient training sessions. Scenarios could serve as a basis to communicate and develop further knowledge within interdisciplinary teams (see Chapter 2.2 for more information). Similarly, stress tests should be developed based on such realistic and appropriate scenarios. Depending on the data availability and data exchange between domains a (partly) automated stress test should be developed. Preconditions, which we have identified for a beneficial data exchange, are listed in Chapter 2.4.

Further develop scenario methodology and use scenario orientation

The main benefit of scenarios is to get a clearer picture of potential future developments and the various ways towards them. This requires an analysis, not only of structural features, but also of inherent dynamical interdependencies and behavioural patterns. This analysis leads to a better orientation w.r.t. future risks, potential impacts as well as strategies to avoid or prevent those risky events.

Scenarios with a special focus on cyber security should be developed in order to cover the most risky or adverse future developments from a top-down as well as a bottom-up perspective. Depicting and assessing contagion effects should be part of these further developments staring from a bird's eye perspective in order to describe direct and indirect cyber security risks. This has been done in ARIEL work package 1 with further refined versions in work packages 3 and 4.

Perform systemic analysis to support the assessment of side and long-term effects and the revelation of risks

Knowledge development and the underlying process of a systemic analysis support the development of a comprehensive and dynamic understanding of complex scenarios. In the course of a situation analysis, relevant actors and elements and their mutual relations are identified and examined, while drawing on a wide range of qualitative and quantitative scientific methods such as System Dynamics, Social Network Analysis, Agent-Based-Modeling, heuristics, etc. In contrast to most other approaches, this one lays an explicit focus on dynamical interdependencies and behavioral patterns. This focus goes

[21] European Central Bank "Cybersecurity for the financial sector", https://www.ecb.europa.eu/paym/pol/shared/pdf/qa_cybersecurity.pdf.
[22] http://www.sesarinnovationdays.eu/files/2015/Presentations/SIDs%202015-EMFASE%20Tutorial%201.pdf.

beyond simply capturing and visualizing a situational picture but rather examines dynamics and trends that may result from certain structures, patterns and delays of the system under consideration. Supporting the assessment of side and long-term effects and the revelation of risks, such a systemic analysis helps to set priorities and to allocate resources and apply instruments efficiently. Moreover, this encourages and facilitates coordination and a "unity of effort" across different ministries, institutions and organizations by providing a holistic approach of analysis and action.

Develop domain-specific attack scenario bases as a service

Besides the development of relevant scenarios and adequate simulations, the development of a knowledge base, which can be used in multiple ways, is a challenging but valuable task, which could be offered as a service. Similar efforts are emerging in the domain of critical infrastructure protection, like the scenario development efforts of the KRIVOR working group of the German UP KRITIS[23].

The service of a knowledge base of attack scenarios can be of use for operational systems, research and teaching for validation, verification and education purposes. Such a knowledge base or management system should be built on basis of a content-server or database which supports the generation and mediation of knowledge, e.g., through visualization. This includes the design and application of a taxonomy, structure, and user interface that meet specific requirements.

Develop relevant scenarios

Clearly, developing relevant scenarios (cf. ARIEL key target) is a major challenge as well as one of the key pivotal points regarding the efficacy of cyber security analysis. With the aid of high-level scenarios, the first steps into cyber security assessment can be facilitated. Then, with the advancements in the appreciation of cyber security in aviation more detailed scenarios of potential attacks can be identified. Further, focusing on different targets of attack from an attacker's perspective helps to identify rational attack pathways or kill chains, as well as irrational but promising ones. The relevance of a single scenario is part of a subjective evaluation of the potential impacts on one stakeholder or a group of them.

Thus, the development of relevant scenarios is not yet finalized with our results in ARIEL. Moreover, a continuous, open and unbiased approach is needed to identify the relevant scenarios. For that purpose, comparable clustering and evaluation techniques with a similar set of indicators helps to build on the set of relevant scenarios which have been developed in ARIEL.

[23] http://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html.

2.4 ENSURE INTEROPERABILITY OF CYBER-RELEVANT MODELS AND DATA

In the aviation sector, there are many different stakeholders with different tasks[24]. While in aviation the development of integrated data and services can be observed[25] a significant share of analyses like safety and security assessments are usually performed in a stove-piped manner based on individual data models. To use data sets for an additional analysis based on other models, at first it is necessary to transform the data in a corresponding format. To avoid overhead of transforming data into the right format it is important to ensure the interoperability of cyber-relevant models and data.

Currently the security analysis in the ATM sector is performed without the use of common and interoperable data models. As a consequence, a computer and tool based exchange and integration of the different analysis results are supported insufficiently. On the other hand, there are many promising efforts for defining common data models which can be used for the security analysis and data exchange in the ATM world as well. Examples are:

- The Structured Threat Information Expression (STIX) data model (together with associated data exchange functionalities called TAXII[26]) has been designed as an XML-model for the description of cyber threats[27].
- The methodology of enterprise architecture models has already been used in the ATM community. The European ATM Architecture (EATMA) is under development.[28] EATMA is based on the NAF[29] (NATO Architecture Framework) meta-model.
- SABSA has been developed as a framework and methodology to meet a wide variety of Enterprise Architecture needs including Risk Management, Information Assurance, Governance and Continuity Management. There are now efforts to integrate SABSA[30] with enterprise architecture meta-models[31, 32].

"Each entity with its own models complicates the interoperability of data"

In the ARIEL project, we used STIX as a basis for the development of the threat model and for the exchange of threat indicators. We also used the EATMA for the definition of the target of attack model. The re-use of available meta-models is imperative for an efficient performance of computer based threat situation analysis, threat data exchange and holistic threat analysis in the future. It is a fundamental precondition for the reusability and standardized application of scenario based analysis, which is shown in Chapter 2.3.

The necessity for the use of standardised data is a distinct result of the development of the threat models as performed in the ARIEL project. If we have not re-used the available models, the effort to define them from scratch would have been too large for the project and the realisation of a tool demonstrator would have been infeasible. The following recommendations show aspects to ensure the interoperability of cyber-relevant models and data.

[24] Air Traffic Control System: Selected Stakeholders' Perspectives on Operations, Modernization, and Structure, Report to Congressional Committees, United States Government Accountability Office, 2014.
[25] ATM Information Reference Model (AIRM) / Information Service Reference Model (ISRM).
[26] http://taxiiproject.github.io/documentation/sample-use/ (last access: 20.10.16).
[27] http://stixproject.github.io/usecases/ (last access: 20.10.16).
[28] https://www.eatmportal.eu/ (last access: 20.10.16).
[29] The NATO Architecture Framework (V3.1) based on TOGAF has no security aspects as well as TOGAF before the integration of SABSA.
[30] Results of the integration of SABSA as a security architecture into the Enterprise Architecture Framework TOGAF are presented at the ARES Conference 2016.
[31] Towards a metamodel for SABSA Conceptual Architecture Descriptions, Patrick Pleinevaux, ARES Conference, Salzburg, 2016.
[32] http://www.sabsa.org/ (last access: 20.10.16).

Develop standardised meta-models

In the future, the use of a set of standardised meta-models is imperative for the computer based data exchange and the development and use of tools for analysis and decision support. For more information, see the model-based analysis approach of Chapter 2.5. The following steps are required:

- Analysis of candidate meta-models and selection of the most promising.
- Adaptation / instantiation of meta-models of the ATM domain (e.g. a STIX scheme for ATM).
- Publication and agreement about the use of the models within the ATM domain (e.g. on the level of EUROCONTROL or even worldwide).
- Collaboration of the responsible standardization organizations to assure that the ATM concerns are taken into account and to support the development and agreement of standards.

Ensure the reusability of data

For the opportunity to reuse data of different sources there is the need for standards concerning:

- Exchange of data containing information about threats, incidents and counter measures (here STIX and TAXII are the most promising candidates which are used in ARIEL as well).
- Enhancements of architecture models used in Air Traffic Management to accommodate security related information i.e. in terms of vulnerability and security respective resilience measures (here enterprise architecture models and SABSA are candidates).
- Assessment of systems and their vulnerabilities in a completely computer readable form.
- Format of data (like XMI in case of Enterprise Architectures).

Develop a standardization of interdisciplinary collaboration

As the possibility is given, the data of a specific domain is interesting for analysis in other domains. Efforts should be made to develop a standardization that can be used across different domains to achieve a better reusability. This process will be accelerated based on interdisciplinary collaboration, which can be facilitated by the measures showed in Chapter 2.2.

Consider organizational aspects

To ensure the interoperability of cyber-relevant models and data, organizational aspects like the following could also be important and should be considered in addition to the findings in Chapter 2.1.

- A Single Point of Contact (SPoC) as an authority to organize a consistent maintenance.
- Release management as a Quality of Service (QoS) of the change and product management.
- Guidelines on how analysts have to evaluate the results of security analysis and security alerts generated by network hardware and applications, so that the reports are comparable and can be used to improve experiences and to train other systems.
- Documentation of used systems to get an overview of the whole landscape.

Recommendation

The project work shows, that the possibility of data exchange is typically supported in an insufficient manner or not at all. If there are interesting data items or results of analysis of other domains, it is relatively unlikely that they are using the same data model. To be able to use the data / results, effort is required to develop an interface for the exchange. But these problems do not only exist across different domains. Sometimes even the same data from different sources are diverging. So, if a dataset is incomplete and it is necessary to enrich it with data of other sources data transformation is needed. To avoid a possible trade-off, it is advisable to develop a standardized model and data format. If a standardized model and exchange format is defined it will increase the reusability of data and results.

2.5 REFINE AND EVOLVE DYNAMIC RISK ANALYSIS METHODS

Cyber threats are a challenge that is now recognized not only by expert communities but also by the broad public, including high-level stakeholders. This leads to a lot of initiatives on different levels in all sectors. Although with a US-centric view, an excellent analysis of the current state of cyber security in air traffic management and control is given by ATCA's Cyber Security Committee, which states that "a comprehensive, holistic, and highly adaptive approach to cyber security is critical to the operations of aviation services in the United States and the world" [33]. Three specific high-level recommendations are proposed (Hardening of systems; Safe connectivity of the community; Operational response), which demand holistic and collaborative approaches in the area of cyber risk and threat assessment, both on strategic / program level and in a cyber security operations context. With respect to the strategic / program level, ATCA's Cyber Security Committee recommends: "Create a research and development process that integrates all systems in aviation to eliminate any interoperability challenges that may be induced by cyber security remediation" [33]. A part of that process needs to be the proper methods and tools to facilitate the integration.

The current practice for the assessment of inventories, architectures and vulnerabilities of organizations mainly rests on manual expert analysis and assessments. Due to the overall size of the necessary assessments, usually many experts generate individual assessments of parts of the overall organization. This work is done manually and is based on subjective evaluations of the contributing experts. Therefore the results are difficult to compare and their integration into a holistic organizational risk management process is difficult, if not impossible.

In the ARIEL project we developed a model-based approach for aviation cyber security risk assessment in support of a holistic understanding of cyber threats and risks in complex interconnected systems. The model-based approach allows a tool-based reasoning which supports a "semi-automated" analysis of risks. This holistic approach, together with the tool support, is supposed to allow the overall modelling and assessment of cyber risks for a large organization or even an assessment of interconnected risks of several cooperation entities (e.g., the European Air Traffic Management system as coordinated by EUROCONTROL).

The main intended applications of the models and tools are *Holistic security analysis of organizations* as performed in a security program context[34] and *Generation of an operational situational picture for dynamical risk analysis* (Dynamic Risk Assessment) as part of day-to-day security operations. As the model-based approach is very general in nature, it could also be used in a security capability maturity modelling approach.

The model based-approach builds on two interconnected types of models: an attack model, which allows inferring the effect of possible cyber-attacks and a target of attack model which allows the propagation calculation of the effects (e.g. concerning the operational activities and capabilities of an organization). This enables an impact assessment, in which the impacts can be associated to the most appropriate elements of the architecture of an organization. The model of attack follows the STIX data model, the model of target of attack and the impact analysis is based on the concept of enterprise architecture modelling (EAM). For the purposes of the ARIEL project, the EATMA was employed as a

[33] ATCA's Cyber Security Committee. (2016, January 1). ATCA Aviation Cyber Security White Paper Series Executive Summary - Forming a Strategic Initiative to Combat Modern Cyber Security Threats. The Journal of Air Traffic Control, 58(1), pp. 37-39.

[34] Holistic security analysis of organizations: This is to be seen as part of the overall cyber security program of an organization or a group of interconnected collaborating organizations. Alternatively, the method should be especially suited to be applied in large-scale R&D programs such as SESAR.

specific example of a comprehensive EAM. Experiences we made with models and data formats led to the conclusions shown in Chapter 2.4.

The requirement of large organizations to improve their ability for identification and prevention of threats was also addressed in the TREsPASS project:

> "Current risk management methods provide descriptive tools for assessing threats by systematic brainstorming. Attack opportunities will be identified and prevented only if people can conceive them. In today's dynamic attack landscape, this process is too slow and exceeds the limits of human imaginative capability. Emerging security risks demand tool support to predict, prioritize and prevent complex attacks systematically."[35]

In this project the "attack navigator" was developed. This navigator enables the user to evaluate which attack opportunities are conceivable, which of them are the most critical and which countermeasures promise to be the most effective for protection and / or mitigation.

The results of the TREsPASS project support our hypothesis, that a tool-based holistic approach will be necessary in the future. Moreover, the project provides complementary tools which could be re-used to complete the toolset of the ARIEL project.

„The dynamic risk analysis method and tool developed in the ARIEL project is a promising holistic approach that is unique in its comprehensiveness"

The dynamic risk analysis method and tool developed in the ARIEL project is a promising holistic approach that is unique in its comprehensiveness. We recommend the continuation of Research and Development work on the method and tool in follow-up projects. Focus should be given on refining and evolving the method with regards to security analysis, online situational analysis and cyber security / resilience maturity assessment, on applying the method to selected real-life use cases as well as on testing the method in additional applications in the area of critical infrastructure protection.

The methods and tools as developed in the ARIEL project have reached the maturity level of a function demonstrator. The next step is the continuing development of the methods and tools in order to reach the maturity level "prototype" and in order to apply this prototype to real life problems using real data. The prototype application shall comprise high priority use cases for *Holistic security analysis of organizations* and *Dynamic risk assessment*. The recommendation comprises several sub-elements presented in the following.

Refine and evolve the methods and tools with regard to security analysis and online situational analysis

This element comprises the technical improvement of the developed tools to the required maturity level. Working steps are e.g. the

- improvement of the Human-Machine Interface (HMI) of the demonstrator based on cooperation with dedicated users and ergonomic experts;
- integration of the methods and tools into the real-world landscape of Security information and event management (SIEM);

Recommendation

[35] https://www.trespass-project.eu.

Recommendation

- completion of the functionality of the methods and tools;
    - Semi-automated aggregation and integration of known technical vulnerabilities of systems
    - Completion of the application of the reasoning technology (Bayesian Networks)
- application of software development standards as required by the dedicated users;
- use of available licensed software tools where appropriate;
- development of a handbook and guideline for the application of the methods and tools.

Research the applicability of the method and tool to the area of cyber security/resilience maturity modelling approaches

This area of application has not been considered in the ARIEL project so far. The general approach of the ARIEL method and tool is supposed to support the analysis of the maturity of cyber security / resilience capabilities. This should be further assessed and tested in follow-on activities.

Apply the methods to selected real life use cases

To be able to validate the benefits of the methods and tools, the prototype must be applied to real world problems using real world data and real-world scenarios (see Chapter 2.3). The application into the real-life use cases requires integrating the application of the tool into adequate processes of the dedicated users.

Transfer the methods to additional applications in the area of critical infrastructure

The risk analysis methods as developed in the project can be transferred to other domains (e.g. critical infrastructure, large companies). This applies as well for the tools which have been developed in the ARIEL project. The requirements and the benefit of the method transfer shall be validated and demonstrated applying them on important domains. The topics of the transfer analysis shall e.g. comprise

- availability of data for the attack models and target of attack model (enterprise architecture),
- availability of organizational elements and processes to use the method and tools.

If the tool support of the approach is realised it will support the risk assessment and the dynamical situational analysis of organisations, which were successful in integrating it into their day-to-day analysis and surveillance tasks and processes.

2.6 SAFETY & SECURITY: ENSURE CONSISTENCY AND ENABLE SYNERGIES

The English expressions *Safety* and *Security* in their day to day usage do not have clearly distinguished meanings and languages like German even have only one word for them (i.e. "Sicherheit").[36,37]

As a consequence, the ways the expressions are used (and translated) in aviation depend on subject context, point of view or "tradition". This is usually reflected in the subject definitions for safety and security, which are notably part of corresponding regulatory and standardization papers.

In aviation security and safety, respectively their management, appear juxtaposed in the regulatory and standardization papers at the global and regional level, i.e. in terms of two separate ICAO Annexes (17 and 19) and related SARP documents (Standards and Recommended Practice), as well as separate provisions in EU regulation[38].

At a high level, commonalities and differences between safety and security in aviation can be summarized in that both form parts of risk management in aviation, which addresses in particular:

- "Unwanted events" in terms of technical failures, acts of god, human error, organizational weaknesses and intentional acts.
- Their potential impact on the key performance areas (KPAs) of civil aviation with a "traditional" focus on the protection of life and limb. However, the overall focus on aviation system performance and its availability as a "critical infrastructure" has widened the view on other performance related impacts.
- The notion of ensuring resilience through preventive, detective and reactive mitigation measures.

Where safety is focused on "system internal" technical failure and human error within the aviation system and their potential impact on life and limb (KPA Safety), security is focused on – externally originated – intentional acts of unlawful behavior with a tradition of dealing with physical threats to aviation, notably in terms of hi-jacking and air terrorism.

During the last decade, it became apparent that:

- The cyber space of the aviation system constitutes a significant dimension for security in terms of threats to availability, integrity and – where applicable - to confidentiality.
- Because of the intentional character of attacks, an analysis of security aspects cannot focus on statistical coherences like many safety-related evaluations.
- Safety and security are both subject to the whole life cycle of the aviation system and its constituents.
- A joint approach may reduce overlaps and increases comprehensiveness by exploring complementary aspects, as well as balancing conflicting ones.
- A holistic view has to be taken towards the resilience of aviation as a socio-technical system, respectively a system of systems (sometimes addressed as a "total systems approach").

A first significant challenge for the achievement of resilience is posed by the fact, that on one side both safety and security management aims for a "steady state" of the aviation system to stay free from

[36] Albrechtsen "Security vs. Safety" (2003) (http://www.iot.ntnu.no/users/albrecht/rapporter/n-tat%20safety%20v%20security.pdf.
[37] Line, Restad, Nordland, Tondel, „Safety vs. Security" (2006). http://ebooks.asmedigitalcolletion.asme.org/content.aspx?bookid=260&sectionid=38776372.
[38] http://eur-lex.europa.eu/summary/chapter/transport/3205.html?root=3205.

harm. On the other side safety pursues the achievement of internal stability ("never touch a running system"), while security recognizes the dynamic – somehow uncontrollable - behavior of the systems environment and requires agility in terms of dynamic monitoring of the relevant influences and timely adaptation of the system and its defensive mechanisms ("fast patches"). This contradiction limits the options for protective measures in safety-focused environments like aviation. Respective conflicts are solved by focusing on efforts to harden the perimeter of a (sub) system, hoping that this could prevent the exploration of (known) weak spots in the core of the system.

A second challenge is posed by the way the evolution of aviation is managed in terms of "improvements". This approach is reflected especially by the modules of the ASBU[39] structure of ICAOs Global Air Navigation Plan (GANP) and correlating regional plan structures like the European master plan's operational changes and infrastructure roadmaps.
The way to think in "improvement-cases" fosters a bottom-up approach of individual, juxtaposed safety and security cases, seemingly unrelated to the integration efforts towards a holistic architecture like EATMA (see the safety and security reference material proposed for the Pilot Common Projects[40] and the SESAR 2020 research endeavors).

A third challenge is posed by the difference in language used. Despite the commonalities of safety and security, differences in safety and security language hinders joint approaches, i.e. in terms of risk assessment and the integration of assessment results. This results in partly double or even triple efforts (if the integration of information in architectural representation is taken into consideration).

The fourth and last challenge concerns the current state of the art regarding the development of aviation (and other modes of transport) which indicates a significant increase of system complexity and dynamics. This applies both to the dynamically changing (aviation) system and its environment, as well as the dynamics of the threat and hazard scenario development. They act as drivers for safety and security as well as a provider of resilience. At the same time market data shows, that respective expertise is – and will remain – a scarce resource. This contrasts with the need to answer the changes notably with dynamic updates of threat assessments and resulting requirement updates. The awareness of these developments drives a growing interest in the exploration of synergies of safety and security integration, i.e. in industrial production and service provision (see e.g. the current harmonization efforts of IEC and the German DKE).

Recommendation

Methodologies applied for safety and security management in aviation should be analyzed for mutual integration options through linkages and complementary elements. Special attention should be given to the following aspects:

- Usage of EATMA's architectural data for analyzing safety and security cases as a joint representation of the different systems and of planned changes. Integration of the documentation and the tracking of safety and security considerations in EATMA. We used EATMA for a model based approach of dynamic risk analysis.
- Evaluation of the comprehensiveness of the EATMA architectural structure to fully appreciate the nature of aviation as a socio-technical system, encompassing "the human factor" as a significant and non-deterministic element of system behavior.
- Exploration of an "all hazards" approach for integrated consideration of technical failures, acts of god, human error, organizational weaknesses and intentional acts.
- Exploration of an "all impact" approach considering all relevant Aviation Key Performance (AKP) areas, in particular safety (signifying the protection of life and limb), capacity and environment.

[39] Aviation System Block Update (ASBU).
[40] http://ec.europa.eu/transport/modes/air/sesar/deployment_en.

- Evaluation and resolution of diversity of “language” used in safety and security (in terms of expressions and semantics) i.e. regarding:
    - (Security) threats vs. (safety) hazards
    - (Security) likelihood vs. (safety) probability
- Comprehensiveness of the methodological portfolios of safety and security throughout the lifecycle (i.e. for risk analysis).
- Determination of measures to be applied in risk mitigation, notably in terms of compliance to existing rules, selection from control and measure catalogues (incl. their adaption for implementation), the application of “best practice” patterns and the need and justification for measure innovation.
- Provision of tradeoff mechanisms for the exploration of synergies and conflicts regarding preventive and reactive risk mitigation measures and their implementation.
- The determination of the aviation system maturity in terms of safety and security, as well as safety and security management.
- Management of “gaps” caused by the incompleteness and inconsistencies of information, notably concerning the aviation system, the hazards and threats and the respective scenarios. For information on data management, see Chapter 2.4.
- Increase in application oriented, coordinated subject information exchange and joint research in the fields of safety and security.

2.7 ENHANCE DESIGN METHODOLOGIES TO ENSURE RESILIENT SYSTEM CHARACTERISTICS THROUGHOUT A COMPLETE LIFECYCLE

Resilience means the continuous adaption of organizational and technical systems (socio-technical systems, resp.) to support their survivability in a changing operational environment. This is driven by the need to guarantee a specific, minimum level of system performance while in operation. To apply a holistic point of view, resilient system behaviour has to be considered not only system wide in an organisational and technical sense, but also considering their planned and dynamically updated long-term changes. In Air Traffic Management, relevant information can be found notably in the ICAO Global Air Navigation Plan and in the European ATM Masterplan.

It is mandatory to consider and to adjust to long-term evolutions, medium-term trends and short-term changes. Long-term evolutions of the overall system and its environment comprise growing air traffic and complexity as well as digitalisation. Examples of medium-term trends or developments are integration of COTS components, the "connected aircraft" or changes of regulatory requirements. Short term, sudden changes typically have negative effects on system performance due to their unexpected and undesired occurrence. These disruptions emerge from human (erratic) actions, technical failures and sudden coincidences. In the worst case, they are caused intentionally, like cyberattacks or physical terrorism. The management of resulting consequences is addressed by resilience as well.

To drive organisational and technical development in a comprehensive way and fulfil the requirements for a continuous, secure and stable system operation, a development approach, based on the principles of "Resilience by Design" has to be established to meet the demands of the permanently and meanwhile rapidly changing operational environment of air traffic systems.

Maintaining resilience in aviation is challenging. The lifecycle of aircraft and other elements of aviation, like ATC systems, has a long duration. The introduction of up-to-date components, which are well adapted to the contemporary operational environment, is systemically delayed for various reasons. A prominent example is the need for diverse elaborate, detailed certification processes of changes to existing systems. The speed of change and increased complexity together with the growing efforts for the implementation of measures to maintain resilience pose a challenge regarding timeliness of risk management in aviation. Without continuous updates and maintenance, systems rapidly start to lose their adaption through a world of ever changing vulnerabilities, threats and environmental conditions.

Regarding the requirements for cybersecurity, the systems face two time-dependent developments, which amplify each other in a dramatic way. Generally, the way cyberattacks are "driven" in the last decade is growing in sophistication. Additionally, due to the inevitable discovery of vulnerabilities of systems over time, the potential attack surface of a non-updated system is growing continuously. In the area of air traffic systems, some vulnerabilities remain existent over decades, due to their isolated operational environment. New interconnections tent to dissolve this protecting separation. Thus, vulnerable systems get connected to current cybersecurity-affected communication systems. Being used as a gateway for cyberattacks, a single corrupted embedded system is enough to put the whole "system of systems" to risk. The increase in complexity of individual subsystems, their interconnections and interdependencies overwhelm conventional, experience-based risk assessment methods.

To react to the current cyber threat landscape and to reduce these potential vulnerabilities in a near term timespan, it is necessary to use occasions like maintenance and repair procedures to replace or upgrade "old", non-adapted components with new ones. The new components are prepared and developed for continuous, functional and security-related maintenance. This approach ensures a step-

by-step integration of newly developed, secure and resilient systems, which will strengthen the overall systems resilience from now on and keep it on a high level continuously in the future.

To meet the demands of a resilient system's properties, the development of the components has to focus on requirements that can be assigned to the three phases of resilience:

- *Protection*, which means the robustness of systems to keep their functionality in the presence of disruptions. The development of protection measures is strongly shaped by the experience through known disruptions and risks (e.g., firewalls or encryption).
- *Mitigation / Survival*, which means the ability of a socio-technical system to actively react on and mitigate unknown disruptions of a system. The most important part of this phase is to ensure the system's survival through foreseeable, controllable and thus stoppable degradation. In complex systems, this means a fault-tolerant behaviour regarding unforeseen interdependencies of systems. Based on an ability to improvise and adapt to new situations rapidly, it is mandatory to develop systems, which empower and assist human beings to find and implement a way to stabilize the system performance or to prevent further loss or failure.
- *Recovery* means the reversal of incurred degradation and the restoration of system functionality. With the integration of the gained experiences in improvements of the implemented solutions for *Protection* and *Mitigation*, both maturity and performance levels of the system grow to a higher level than before, if the system is designed to accept updates.

Due to increasing interconnections, there is a growing complexity of the overall system, which drives the principle of reductionism and the independent optimization of particular systems to its limits. For a comprehensive view of resilience engineering it is necessary to consider the functional interdependencies of subsystems and potential cascading effects in case of their failure. Additionally, mutual interdependencies with the human user have to be considered for both cases: failure and mitigation.

While today's resilience engineering has a strong focus on coping with unintentional acts like technical failure and human error, a broader view is required to be also prepared for intentional acts like cyber-attacks and sabotage.

An example for a security mechanism on the physical layer, which was developed by the German Aerospace Center (DLR), is a phased array antenna which serves as a GPS-receiver.

Phased array antennas have strong directional signal distribution characteristics, which enable them to physically filter spoofed signals from "wrong" positions by constructional design. Based on the received signals, they are able to conclude the position of the sending entity and thus are equipped to detect anomalies on a logical level. The GPS antenna was constructed to meet the typical size of traditional GPS antennas and therefore, it is possible to replace existing receivers including the antenna without changing any aircraft equipment. This example shows a possibility of how to strengthen resilience of the overall system by replacing old components with new ones, which are adapted to actual needs of their operational environment. The antenna array protects through physical filtering. It enables mitigation in the moment of anomaly detection and helps to recover from an attack / failure by providing redundancy and diversification.

Another example for a resilient system architecture chosen in ARIEL is the surveillance data stream. Its major purpose is to serve air traffic controllers as an "electronic eye", which provides a situational picture of the airspace under control. One of its main components is the individual radar device, which needs to be resilient in terms of availability and the integrity of the information it provides. This is where resilience design needs to be applied at the element level. The ARIEL example deals with the

achievement of resilience related to threats caused by electromagnetic impacts (e.g., spoofing or jamming).

While design at the individual radar device level may improve its resilience, it is clear, that protective measures find their limits. Therefore, the overall design needs to consider the application of multiple, overlapping radar sensors. Furthermore, a diversity of surveillance sensors beyond radar can be applied to empower the overall system to mitigate a loss / failure of one radar station through reallocation of resources based on the suitable application of redundancy and diversification.

Tying the sensor data into a network of data transport connections and systems, responsible for the fusion of the arising multitude of sensor sources, adds a layer of complexity and potential vulnerability. This in turn requires the design of protective, detective and reactive measures, which need to address both, the individual elements and their orchestration in terms of diversity and alternative network connections.

The ultimate design challenge addresses the secure orchestration of the overall data stream and its users. This challenge asks for early detection of emerging failures to provide time for emergency and continuity measures, taken by the users, up to the organizational procedures to initiate the clearance of air spaces, where the loss of the "electronic eyesight" is unavoidable. Design in that respect addresses the integration of technical constituents with organizational procedures and the humans in terms of controllers and supporting technical staff.

The resulting complexity introduces meta-vulnerabilities notably in terms of uncovered flanks and gaps in the overall system and the impact of the non-deterministic behavior of the human beings. It is obvious that this complexity needs to be made visible during analysis in order to provide a stable requirement basis for the design of the appropriate security measures respective the measure orchestration.

Following the method of resilience engineering within the ARIEL Project and applying it exemplarily to air traffic systems and its architectures with respect to cyber resilience, we found the following recommendations:

Recommendation

Enhance design methodologies to ensure resilience throughout the complete lifecycle

Include demands of cyber resilience in the process of creation, operation and maintenance of air traffic systems. Measures of cybersecurity aim mainly at protective developments. Since overthrowing these measures is a matter of time and effort, it is mandatory to consider the functions for mitigation and recovery in the same way while developing systems and processes.

Analyse system complexity and interdependencies

The aim to improve the business performance drives the integration of the systems used. It results in a growth of complexity and interconnections at a fast pace. A balanced development, which considers resilience (technical & functional) as well as safety and security will enable long-term success and correct a destabilising trend to focus on creation of systems and functions without considering complexity issues and interdependency effects.

Integrate cyber-resilience and functional needs into low-level health monitoring systems

A prerequisite for the achievement of resilience is the knowledge and understanding of the diverse system states of its elements at each point of time. Therefore, system self-monitoring on the level of technical system components is a fundamental prerequisite for resilient behaviour of the overall system. It is the basis to recognize a breach in protection measures and to find a suitable and situation-specific mitigation strategy within dynamic risk assessment, like proposed in Chapter 2.5. Indicators

for system status and performance help to evaluate the efficacy of mitigation and recovery measures. Analysis and assessment of stored data enable growth of experience regarding system behaviour and can be used as a real-world data basis for scenario development, as described in Chapter 2.3. For interdisciplinary teams, monitoring data serve as a source of information to recognize inter-domain linkages and coherences (see Chapter 2.2).

Identify mitigation strategies for complex systems with dynamically changing architecture

A dynamically changing, complex system architecture is difficult to control. Methods, approaches and models like EATMA have to be further developed in order to give orientation while creating strategies to mitigate disruptions for even more complex systems in the future. For a model-based approach to cyber risk analysis, see Chapter 2.5.

Include principles of resilience into technical developments in a comprehensive way

In the presence of contradictions, assure efforts on resilience, efficiency and performance at a comparable priority level. Even a super-efficient air traffic system has to be resilient. In case of an attack or disruption, it must not produce performance variations through sensitive degradation behaviour and / or contagion effects.

Consideration of resilience in all phases of a potential incident

Measures based on the phase of protection:

- Find a suitable balance of redundancy and diversification to bring a system of systems to an optimal level of robustness.
- Find protection mechanisms on physical, functional and operational levels of a system (e.g. physical: directional antenna vs. spoofing; functional: redundancy, diversification; operational: human factor, authentication).
- Ensure redundancy of critical systems, e.g. complement navigation based on Global Navigation Satellite Systems (GNSS) with Alternative Positioning, Navigation and Timing (APNT) means for cross verification and validation.
- Create systems, which are able to keep their protection level through updates and maintenance.

For strategies in the mitigation phase, we see the following issues:

- Make sure systems performance variability is controllable in presence of disruptions to enable slow, predictable degradation behaviour.
- Keep a high level of awareness and training since target oriented, successful acting in unknown situations is based on experience. Enable human operators to deal with interdependencies in complex, inter-domain systems (no “turning off/on” of black boxes, but implementation of mitigation strategy). You can find more information on how to manage interdisciplinary teams in Chapter 2.2.
- Utilize (future) capabilities used for autonomous or highly automated systems to assist a human being while preventing or mitigating disruptions in complex system environments.
- Avoid critical data paths by ensuring redundancy and diversification, e.g. by distributing Ground-Based Augmentation System (GBAS) and Satellite-Based Augmentation System (SBAS) correction data via the future L-band Digital Aeronautical Communications System (LDACS), in addition to GBAS VHF Data Broadcast (VDB).

Recommendation

- To meet the resilience requirements caused by growing system complexity, refine methods and capabilities of autonomous or automated systems to enable simple mitigation by the systems themselves, e.g. self-healing capabilities.
- Find methods and processes to dynamically adapt technical and operational resource allocation within systems to reduce the impact of the disruption.

Resilience in the Recovery phase is a chance to improve the resilience of the overall system:

- Collect and analyse data to ensure best improvements and documentation.
- Refine and develop methods for dynamic resource allocation to enable in operation recovery and fluent reintegration of systems after recovery.
- Enable systems to renew / recover through in-operation installation of backups.
- Based on system-health monitoring: allocate resources balanced in regards to subsystems performance needs (redundancy / diversification) to enable stabilization and recovery of systems.
- Add flexibility to information dissemination and increase coverage, by enabling air-to-air communication.

2.8 EXPLOIT SIMULATION METHODOLOGIES TO SUPPORT CYBER THREAT AND RISK ANALYSIS OF COMPLEX SYSTEMS

In the holistic approach of cyber threat and risk analysis of ARIEL (see Chapter 2.1), we were concerned with question like the following:

- What are the concrete effects of a cyber-attack to subsystems or processes, which are identified by cyber threat and risk analysis?
- What happens if certain data is modified or temporarily unavailable due to an attack?
- How do effects propagate in a system in time and space and where and when do conceivable system changes occur?
- How critical are the effects of potential integrity violations of data and is the system able to return to a stable operational state?

Alongside other approaches, we evaluated simulation methodologies to address these questions. Simulation gains its importance for ATM by the fact that there are only limited options for real life experiments in this domain. The aim of our activity was to investigate the suitability of this methodology in the context of cyber threat and risk analysis. We simulated a subset of the ARIEL scenarios where the integrity and the availability of flight plan data is impacted by deliberate cyber-attacks. One scenario characterises an attack on the integrity of flight plan data, assuming an intentional manipulation of the cruise flight level (Level Capping Scenario). In a second scenario, the attack compromises the availability of flight plan data. We assumed that flight plans with departures in Munich are intentionally deleted in the central ATM systems used to distribute flight plans to the responsible ATC units.

In the context of these scenarios, we demonstrated that marginal manipulations can have significant influences on the overall system behaviour. We observed notable increases of delays and fuel consumption, even with the potential of provoking air safety incidents. We showed that a few deleted flight plans have a significant impact on the overall system operation. For example, the deletion of only five flight plans lead to a dramatic increase of averaged delay for arrivals and departures.

We are confident that simulation can be broadly applied to support threat and risk analysis in a cyber-security context. In general, simulation experiments allow the observation of the behaviour of a system in different settings and situations. Our research indicates that this statement is valid for cyber-security concepts and strategies interacting with a simulated environment and is valid for modelled real world systems dealing with simulated cyber-threat situations, as well.

Our simulation activities also had to face common problems frequently encountered in simulation-based studies, such as collection, verification, and review of necessary data to develop simulation models and scenarios. We propose that appropriate funding for the compilation of the data needed for simulation is included in future simulation projects with similar needs. Furthermore, we suggest simulation as methodology to provide data, i.e. as a source for subsequent security research or as input for decision support in security management.

Simulation as an established methodology to investigate and evaluate complex systems can help to increase the understanding and assessment of the impacts of potential cyber-attacks. Furthermore, it creates a reliable basis for mutual understanding of experts from different domains and disciplines[41].

[41] R. Markus, S. Spieckermann und S. Wenzel, Verifikation und Validierung für die Simulation in Produktion und Logistik: Vorgehensmodelle und Techniken., Springer Science & Business Media, 2008.

As an example, we frequently experienced positive feedback from operational staff when demonstrating our cyber threat scenarios with the help of simulation.

Recommendation

Develop, maintain and apply simulation models and cyber-attack simulation scenarios

To achieve a holistic understanding of the effects of potential cyber-attacks in complex systems, simulation is a valuable method to complement more traditional analysis methods. We recommend a more widespread application of simulation models for processes and systems identified by cyber threat and risk analysis as critical for the system operation. Simulation increases the understanding of the impact of identified cyber threats and supports the validation of risk analysis results. The increase in understanding of impacts and effects is the basis for the development of effective countermeasures, for example algorithms and methods for early warnings about potential cyber-attacks.

Additionally, we recommend to maintain and to use existing simulation models for cyber-threat and risk analysis. Our research shows that simulation models of airborne processes do not necessarily need a special design to support a wide range of experiments regarding cyber-attacks. We assume that this observation is valid in other domains outside the aviation sector, as well. A simulation experiment is based on scenarios where the specific data manipulation has to be identified and specified. Therefore, it is important to develop valid simulation scenarios. Interdisciplinary teams that are able to provide a comprehensive consideration of attacker motivation and attack impacts should develop these scenarios (see also Chapter 2.2 and Chapter 2.3).

Furthermore, we recommend using simulation results for cyber-security awareness building, especially for task-specific security awareness trainings. Beyond basic awareness, simulation can also be exploited to support decision-making and planning processes, by exposing decision makers and planners to the data produced by simulation.

Connect and develop simulation models "from gate to gate"

Most existing simulation models focus on a special area of application. Potential propagations of effects across the boundaries of individual operational processes are usually difficult to observe and analyse. For example, the evaluation of the impacts on ground processes or strategic planning processes resulting from a cyber-attack to the overall chain of processes needs integrated and connected simulation models. We recommend to identify, to specify, and to develop the needed connections across simulation model boundaries.

Integrate human interactions with cyber-attack simulation scenarios

Beyond the closed-loop simulation without user interaction applied in the ARIEL project, Human-in-the-Loop simulation (HITL) needs to be applied to examine human factors aspects of cyber resilience. In this context, HITL simulation is essential for getting direct feedback in simulated live situations from operational staff with respect to cognition of and reaction to potential cyber-attacks. In the case of closed-loop simulation, typical user interactions need to be modelled with assumptions or simplifications. Especially in the area of air traffic management and flight execution, the assumptions on these interactions influence the results of a simulation significantly.

We recommend integrating human interactions within cyber-attack simulations to increase the validity, quality, and significance of the simulation results and to study and observe the behaviour of humans interacting with a system under cyber-attack. For example, the execution of cockpit and ATC workstation simulation allows the measurement of negotiation, reaction and action times. It requires the staffing of the simulations with personnel with operational skills. This will improve existing simulation models and support the development of new models. Moreover, the results of HITL simulations

will support the identification of security requirements for systems in aviation that are susceptible to potential cyber-attacks. The simulations will also provide input to the currently ongoing discussion about essential future skills of operational staff that are needed to identify and manage cyber-attacks.

Since HITL simulations are also prevalent in the area of education and training, we recommend integrating cyber-attack simulation scenarios within these training programs to support and improve the development and implementation of codes of conduct to face potential cyber-attacks.

3 CONCLUSIONS

As the recent development shows, the number of cyberattacks is raising in various domains. The level of sophistication and professional implementation leads to the assumption that there is a vital development and collaboration within the attackers' scene and a busy, interdisciplinary exchange with non-hackers on the operational side of this criminal business. Beside financial interests, attacks on critical infrastructures have lately become an instrument of political threat and suppression. Considering the level of professionalism, it is a matter of time until an offense in the aviation sector succeeds. These threats put critical infrastructures, and especially the air transportation system, persistently to risk.

Cybersecurity is not to be seen as an absolute, merely technical capability, but rather has to be perceived as an ongoing, holistic effort to protect an organization and its diverse systems from damage through cyberattacks in a comprehensive way. Additionally, in domains like air transportation with tight collaboration of various organizations and stakeholders in a "system of systems", it is essential to drive a continuous and all-embracing program to keep cyber resilience at a high level, which includes active cooperation of all members of the overall system.

The ARIEL project's holistic approach resulted in eight key recommendations, which we think are of vital interest to strengthen the air traffic systems cyber resilience.

For a sustainable effect, we see the need to further develop specific methods of interdisciplinary, intra- and inter-organizational collaboration in the field of cyber-resilience. For this reason, scenario techniques should be established as a pivotal point of cooperation, as they enable different views of all team members on the "same" system. Based on a library of standard scenarios, which have to be established, a framework for research and development, implementation and validation could be the basis of large-scale exercises, ensuring comparable results. For a vital exchange of knowledge and an efficient operational cooperation, cybersecurity-related data formats and information structures have to be standardized by international authorities. Existing types of data models have to be further developed, as they have to fulfil multiple, domain-specific requirements. This is an essential aspect, because it is the basis for a continuous, dynamic risk analysis, which is a prerequisite for a high level of resilience within an overall system. After further development, the model-based approach of the dynamic risk analysis in the ARIEL project will allow establishing an online, dynamic and tool-based decision support to mitigate disruptions of systems. Simulation methodologies can be applied in addition to other approaches to improve understanding of dynamic effects and human factors in the context of cyber-attacks and to serve as the basis for security awareness building.

As both safety and security are drivers for the determination of resilience requirements it is sensible to take an integrated view on both subjects to foster the consistency of resilience concepts in aviation.

The domains of air transportation and cybersecurity are organized with a strong focus on protective mechanisms, in terms of their operational and technical implementation. To fulfil the requirements of continuous adaption to keep a high level of cyber resilience, the architectures of operational and technical systems have to be restructured based on the results of persistently executed risk analysis. According to that, we strongly recommend to balance the cost- and performance-driven development and prioritise a sustainable, comprehensive and continuous improvement of the overall systems cyber resilience.

GLOSSARY

Aviation System

The Aviation System comprises the participants manufacturer/supplier; Maintenance, Repair and Overhaul (MRO); Airlines; Air Navigation Service Providers (ANSP, Survaillance); Airports; Regulation; Air Traffic Management

Chief Information Officer (CIO)

A Chief Information Officer carries responsibility for the strategic and operational leadership of Information Technologies within institutions

Chief Information Security Officer (CISO)

A Chief Information Security Officer ensures, that information- and technology-related assets are protected from harm, is responsible to enhance structures and processes continuously to reduce IT risks and – in case of an incident – mitigates the impact to lower damage.

Cyber operational resilience

Based on the definition of resilience, cyber operational resilience focusses on resilient capabilities of cyber-physical systems within their operational environment.

Cyber risks

Cyber risks are of complex nature and domain specific. They describe the risk of loss, disruption or damage to an organization, originating from its IT-systems, which is caused unintentionally or on purpose.

Cyber security capability maturity model (C2M2)

Based on a Cybersecurity Capability Maturity Model an evaluation reveals not only an organizations cybersecurity capabilities, but assesses the sophistication und sustainability of its cybersecurity program. The aim is to develop knowledge about the effects of policies, processes and procedures, which have direct influence on an organizations cybersecurity posture. Maturity Indicator Levels (MILs) constitute an initial position for the development of operational and management strategies considering both, normal and crisis modes of operation.

Cyber Threat Indicator

Indicators convey specific observable patterns (may) combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context.

Domain (in the ARIEL context)

See Air Traffic Domain.

Dynamic Risk Management

Threat landscape in the Cyberspace is changing continuously. Therefore a dynamic, continuous approach for cyber risk management is needed, to provide tool-based decision support on-time for the mitigation of threats.

Information Security Management System (ISMS)

An Information Security Management System (ISMS) is a set of processes and regulations, which supports the continuous maintenance of information security within institutions. An ISMS comprises the definition, control and ongoing servicing and improvement of technical and organizational measures.

Kill Chain

Assuming that attacks occur in stages, a kill chain model identifies the steps of an intrusion. Defense is orientated at this stages.

Resilience

Resilience is seen as the ability of a system to absorb or avoid damage without suffering complete failure. It integrates the aspects of protection, mitigation and recovery. The objective of protection is the achievement of robustness, i.e. the ability of a system to work as intended, although there are disturbances. Protection is complemented by mitigation, which in aviation pursues a graceful, stepwise degradation of the services, whose robustness can no longer be guaranteed (e.g. the fall

back from auto-piloted to manual flying). Recovery, as the ultimate element of resilience, pursues the (stepwise) restoration of the capabilities of a system.

Stakeholder in the aviation sector

In the ARIEL project we defined stakeholder groups in orientation to the SESAR definition. Airport operators (APT); Airspace Users (AU); Air Navigation Service Providers (ANSPs); Network Management (NM); National Regulatory Authorities (REG); Military (MIL). Additionally we identified the groups Manufacturer/Supplier (+maintenance of products); Research & Development, which includes Research Funds; Research Strategy Management

ABBREVIATIONS

ACI ..... Airports Council International
AKP ..... Aviation Key Performance
ANSP ..... Air Navigation Service Providers
APNT ..... Alternative Positioning, Navigation and Timing
ARIEL ..... Air Traffic Resilience (project name)
ASBU ..... Aviation System Block Upgrade
ATC ..... Air Traffic Control
ATCA ..... Advanced Telecommunications Computing Architecture
ATM ..... Air Traffic Management
BDL ..... Bundesverband der Deutschen Luftverkehrswirtschaft
C2M2 ..... Cybersecurity Capability Maturity Model
CANSO ..... Civil Air Navigation Services Organization
CDO ..... Chief Digitalization Officer
CEO ..... Chief Execution Officer
CERT ..... Computer Emergency Response Team
CIO ..... Chief Information Officer
CISO ..... Chief Information Security Officer.
DKE ..... Deutsche Kommission Elektrotechnik
DLR ..... German Aerospace Center
EAM ..... Enterprise Architecture Modell
EATMA ..... European Air Traffic Management Architecture
ECB ..... European Central Bank
GANP ..... Global Air Navigation Plan
GBAS ..... Ground Based Augmentation System
GNSS ..... Global Navigation Satellite System
GPS ..... Global Positioning System
HITL ..... Human-in-the-Loop
HMI ..... Human Machine Interface
IATA ..... International Air Transport Association
IEC ..... International Electrotechnical Commission
IT ..... Information Technology
KPA ..... Key Performance AREA
KRIVOR ..... (szenario-basierte) Krisenvorsorge
LBC ..... Ludwig Boelkow Campus
LDACS ..... L-Band Digital Aeronautical Communication System
LOT ..... LOT Polish Airlines
LÜKEX ..... LänderÜbergreifende Krisenmanagementübung (EXercise)
MIL ..... Maturity Indicator Level

MNE7 ..... Multi-National Experiment 7
MRO ..... Maintenance Repair and Overhaul
NAF ..... Nato Architecture Framework
OCTAVE ..... Operationally Critical Threat, Asset, and Vulnerability Evaluation
PDCA ..... Plan-Do-Check-Act
QoS ..... Quality of Service
R&D ..... Research and Development
SABSA ..... Sherwood Applied Business Security Architecture
SARP ..... Standards and Recommended Practice
SBAS ..... Satellite Based Augmentation System
SEI-CERT ..... Software Engineering Institute - Computer Emergency Response Team
SES ..... Single European Sky
SESAR ..... Single European Sky ATM Research – Joint Undertaking
SIEM ..... Security Information and Event Management
SPoC ..... Single Point of Contact
STIX ..... Structured Threat Information Expression
TAXII ..... Trusted Automated eXchange of Indicator Information
TREsPASS Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security
U.S. ..... United States [of America]
UP KRITIS ..... UmsetzungsPlan KRITische InfraStrukturen
VDB ..... VHF Data Broadcast
VHF ..... Very High Frequency (communication)
XMI ..... XML Metadata Interchange
XML ..... Extensible Markup Language

For further informations, please contact:

Tel. +49 89 6088-2281
ariel@iabg.de
www.iabg.de

Supported by the
Free State of Bavaria

LUDWIG BÖLKOW
CAMPUS
AEROSPACE | SECURITY

IABG
Einsteinstraße 20
85521 Ottobrunn
Tel. +49 89 6088-2030
Fax +49 89 6088-4000
info@iabg.de
www.iabg.de