A Model-Based Approach for Aviation Cyber Security Risk Assessment

Tobias Kiesling, Josef Niederl, Jürgen Ziegler
IABG mbH
85521 Ottobrunn, Germany
e-mail: {kiesling, niederl, zieglerj}@iabg.de

Matias Krempel
Deutsche Flugsicherung DFS
63225 Langen, Germany
e-mail: matias.krempel@dfs.de

***Abstract*—The air transport infrastructure is an attractive target for cyber attacks due to its importance and prominence. The current system is already vulnerable and the advent of more automation and pervasion of standard IT in the future leads to ever more complex and interconnected systems with an increasing attack surface. To cope with this situation, we need suitable methods and tools to achieve understanding of the consequences in potential cyber threat situations. We propose a model-based approach for aviation cyber security risk assessment in support of holistic understanding of threats and risk in complex interconnected systems. We introduce our modeling approach and show how computer-based reasoning can be used for threat and risk analysis based on these models. This paper presents the promising results of initial research. Substantial effort is still needed to mature the approach. We expect major challenges to be of an organizational rather than technical nature.**

I. Introduction

Cyber security in all its facets is not a new issue. It has been considered in various aspects for quite a long time, typically with a focus on technological aspects. Nowadays, it is largely recognized, that among other effects, cyber threats could be targeting critical infrastructures such as energy supply, telecommunications, or transport. Air transport as part of the transport critical infrastructure is an attractive target, both in terms of its publicity as well as its importance. This is reflected in increased efforts to define and implement necessary security measures, especially in the context of air navigation service provision [1].

We will use the term Aviation Cyber Security to encompass all viable protective measures against potential cyber threats targeting the global air transport system or parts of it. We will further differentiate between preventive measures (intended to prevent threat actors to successfully infiltrate systems) and resilience measures (limiting the effectiveness of successful intrusions). It is a matter of ongoing debate whether the current air transport system is effectively protected against cyber attacks that can result in aircraft crashes or similar catastrophic events. However, there are other types of cyber threats in air transport that have materialized (e.g., the actual incidents in Warsaw [2] and the US [3]).

The advent of modern technology is manifested among others in the development of the next generation of ATM systems (in Europe especially towards a Single European Sky through the SESAR program) as well as ever more thoroughly interconnected and automated systems. These trends are positive in terms of the improvement of stakeholder experience as well as the increase in efficiency and capacity of the overall air traffic system. On the downside this unfortunately leads to an ever increasing attack surface, as well. To cope with this situation, we need effective risk-based approaches to security. Unfortunately, classical risk assessment methodologies employed in the context of information security are not well suited for complex interdependent system-of-systems analysis. The first and foremost challenge here is the understanding of air traffic as a functional system integrating people, rules and technical systems. A holistic approach has to consider all essential sub systems and their interdependencies in the context of potential threat situations. What we need as basic building blocks are proper methods and tools for a holistic threat and risk assessment.

In this paper we introduce a model-based approach for aviation cyber security risk assessment. It is aimed at supporting a holistic understanding of the threat and risk situation in complex interconnected systems of critical infrastructures such as the air traffic system as a whole. We combine different well-accepted methods for the generation of a risk model which captures all aspects of cyber threats in air traffic. The model shall be usable to perform a dynamic risk analysis not only from a system view point but also from an operational and capability view. The basic idea is simple: The success of a cyber-attack against elements of the air traffic system of systems will result in degradations at all levels of the system which could eventually result in impacts like loss of passenger and freight transport capacities, degradation of operational efficiency, reputation and eventually business. We therefore defined a model which comprises three sub-models, an attack model, a model of the target of attack and an impact model. The models are linked via elements derived from an enterprise architecture, which are part of the linked sub-models. The approach is based on approved standards: the Structured Threat Information eXpression (STIX) [5] for the attack model, Enterprise Architecture for the target of attack model and the impact model, reasoning under uncertainty using Bayesian Networks within the attack model and using enterprise architecture relations within the target of attack model.

The next section introduces the most important building

978-1-5090-0990-9/16 $31.00 © 2016 IEEE
DOI 10.1109/ARES.2016.63

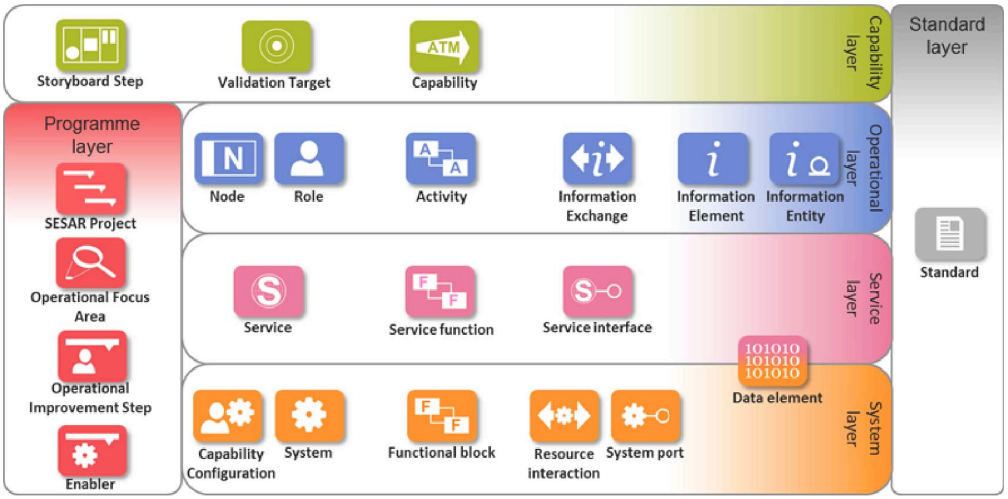

Fig. 1. EATMA Meta Model [Source: [4]]

blocks that we employ as part of our combined methodology, including an analysis of related work for each building block. The methodology itself is presented in Section III. Section IV discusses some aspects of the practical evaluation of the method. Finally, Section V concludes the paper and indicates directions of future work.

II. Technical and Methodological Foundations

The most important building blocks comprise the approach of enterprise architecture modeling and specifically the European ATM architecture, risk assessment methods, especially in the ATM domain, the STIX data format for threat information sharing, as well as the methodology of Bayesian networks.

A. Enterprise Architecture Models and European ATM Architecture (EATMA)

Enterprise architecture models (EAM) [6] are increasingly used to represent and analyze enterprises concerning their systems, their operations, their services and their capabilities using different views. Currently, there are no provisions for incorporating risk analysis directly in the model. However, an EAM describes the elements of an enterprise which could be targets of potential attacks. This can also be exploited to analyse enterprise risks related to degradations or disruptions of those elements.

The European ATM Architecture (EATMA) [7] provides a model of the current state and evolution of air traffic management (ATM) in Europe. It integrates the different improvements undertaken in Europe in support of the global air navigation plan of the International Civil Aviation Organisation (ICAO) [8], respectively its supporting aviation system block upgrades (ASBU) framework [9]. The EATMA is build on the NATO architecture framework (NAF) version 3.1 [10]. For illustration purposes, the meta model of the EATMA is presented in Figure 1.

In simple terms the EATMA consists of an operational architecture representing the air traffic management activities for flight handling and a technical architecture that describes the technical ATM systems including supporting meteorological, communication, navigation and surveillance elements. The EATMA shows the relationship of involved parties – notably civil and military airspace users, airports, air navigation service providers (ANSPs) and meteorological offices. It links technical elements to operational activities.

One of the actual weak points of EATMA and NAF 3.1 is the absence of a security (sub)-architecture in terms of security activities and systems [11]. While EATMA is an on-going development, it has the potential to serve as a kind of a *map* of ATM for the purpose of security risk analysis. Planned EATMA improvements that are relevant for cyber security includes the completion of the interlinks between technical and operational architecture showing the relationships between technical elements and operational activities.

B. Risk Assessment in the ATM domain

Security in aviation is traditionally based on the respective provisions of ICAO, notably its annex 17 [12]. Up to the end of the cold war security in air traffic management was part of the overall security responsibility of the nation states as the owners of their national air traffic management government agencies. It used to be based on internal approaches and focused in line with the respective version of ICAO Annex 17 on physical security. Privatization of ATM and the emerging application of standard ICT equipment required new approaches for an integrated view on physical and IT-security. Respective cyber security risk assessments were carried out since last decade of the 20th century using best practice methods, like the German IT-Sicherheitshandbuch [13]. Since the beginning of the 21st century emerging cyber security norms like ISO 27005 provide frameworks for the alignment of such methods.

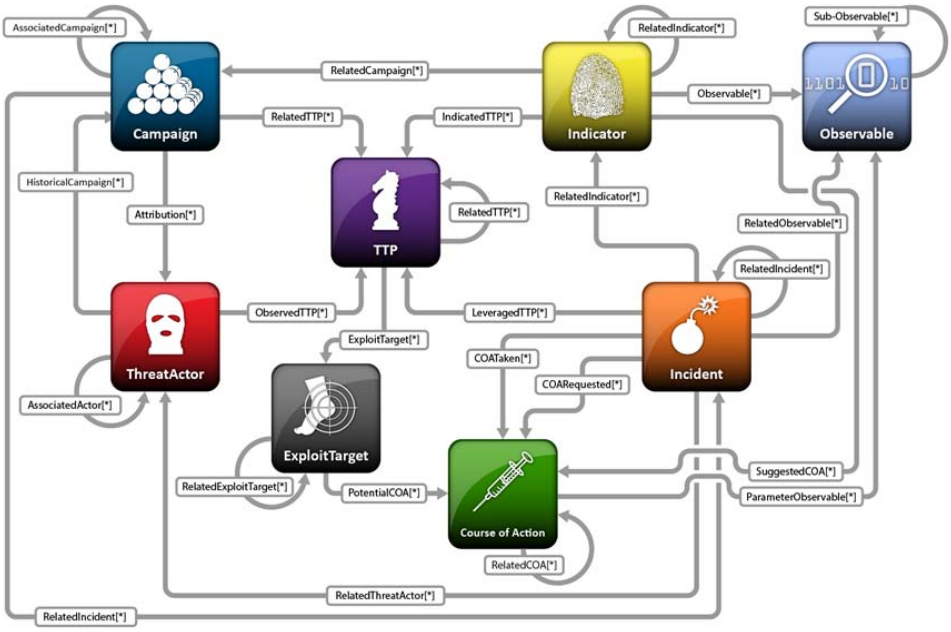

Fig. 2. STIX Architecture [Source: [5]]

The introduction of Single European Sky legislation included formal rules for security driving a more systematic approach including security risk assessment [14].

Generally risk is calculated from the combination of the likelihood of undesired states of the regarded system and the impact/damage which results if this undesired state has occurred. To determine the likelihood of an undesired state, the possible reasons of its occurrence have to be assessed regarding issues like probability of accidents or – regarding a cyber attack – know-how, equipment, vulnerabilities of the target and so on. The impact assessments have to be applied to criteria which are significant in the ATM domain. For instance, these could be monetary (e.g., loss of earnings, recovery/repair costs and personnel costs), danger of life and limb (e.g., injuries or death), loss of intellectual property or brand value, loss of trust, environmental damage, or legal consequences (e.g., violation of contracts, data protection laws or international law). For the development of our methodology we decided to apply expert assessments to the elements of the EATMA using appropriately selected assessment criteria.

For the purpose of the SESAR development phase SecRAM [15] was compiled as a tailored security risk assessment method. It was meant to be applied in the different operational focus areas of SESAR[1]. While the method proved to be feasible at the level of the individual operational focus areas, the integration at the overall ATM level and the maintenance throughout the ATM life cycle beyond SESAR is still seen as an issue [11]. For onboard system security a parallel development based on EUROCAE WG 72 [16] and RTCA SC 218 [17] was carried forward, pursuing a framework in support of aircraft certification.

While a unification of the risk assessment approaches mentioned above might not be feasible due to subject specific and cultural differences, interoperability of the assessment results is required in support of an overall “ATM security case”. This includes notably a common understanding of impact and likelihood criteria as well as risk evaluation and acceptance criteria [18].

C. Structured Threat Information eXchange (STIX)

STIX [19] is a data format (or XML-based language) being developed in collaboration with interested parties. It is intended for the specification, capture, characterization and communication of standardized cyber threat information. Its aim is to support more effective cyber threat management processes and application of automation [5]. The STIX data model identifies the core cyber threat concepts as independent and reusable constructs and characterizes all of their interrelationships based on the inherent meaning and content of each element (see Figure 2). The threat actor element is a characterization of malicious actors representing a cyber attack threat including presumed intent and historically observed behavior. Observables describe what has been seen or might be seen in the cyber space. Indicators describe patterns for what might be seen and the related meaning. Incidents describe instances of specific adversary actions. Tactics, Techniques and Procedures (TTPs) describe attack patterns, malware, exploits, kill chains, tools and other methods used by the

[1] An example can be found under http://bit.ly/1XHY77O

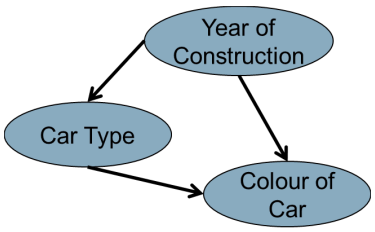

Fig. 3. Simple Bayesian Network

adversary. Exploit Targets describe vulnerabilities, weaknesses or configurations that might be exploited. Campaigns describe sets of incidents and or TTPs with a shared intent. Courses of Action describe actions that could be taken in response to an attack or as a preventive measure. We used the STIX data model as a starting block for the definition of the semantics of our model of attack. Additionally we directly re-used several concepts of the STIX model within that model. As illustrations of STIX messages, so-called STIX idioms can be found on the STIX web pages [20].

D. Bayesian Networks

Bayesian Networks (BNs) provide a natural and efficient way to represent causal models together with uncertainty [21]. The various elements of a domain with their inherent states are represented by nodes of a graph. The causality is modeled as the edges of the graph and the uncertainty between dependent nodes is quantified by so-called conditional probability tables. A simple example in Figure 3 illustrates the principle.

The probability that a car has a specified color will usually depend on the type of the car (the red Ferrari) and the year of construction (whether a color is fashionable). These dependencies can be modeled by conditional probabilities, e.g. $p(\text{red}|\text{Ferrari}) = 0.9, p(\text{red}|2015) = 0,062$. All combinations of cars, years and regarded colors determine the conditional probability tables for this simple model. This BN supports the following reasoning types of *analysis* ("Assumed a car was built in 2011, what is the probability that it is yellow?") and *evidence* ("I observed a yellow Ferrari, what are the probabilities of the possible years of construction?").

Bayesian Networks are applied to different types of problems incorporating risk and safety assessment [22]. Examples among others are analysis of crime risk ([23], [24]), reliability analysis in safety critical environments [22], terrorism risk [25], credit-rating [26] and probability of default [27] for large companies. BNs are also used for analysis of some aspects of ATM applications [28] as well as of cyber security analysis [29], [30]. Recently, BN were employed to assess cyber threats in the ATM area [31] to identify the existence of the adversary, his intention and the level of competence. We used BN to assess potential threats regarding all aspects of an attack following the STIX meta-model.

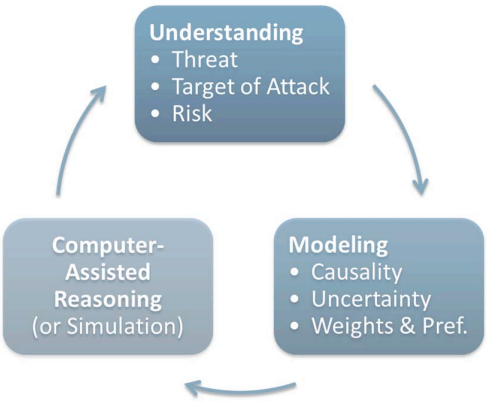

Fig. 4. Application of the Approach

III. A Model-Based Approach for Aviation Cyber Security Risk Assessment

The general problem set addressed in this paper is the generation of understanding of the threat and risk situation in the overall aviation system of systems. We propose an approach that can be used in an application triad of understanding, model generation and maintenance, as well as reasoning (either using artificial intelligence methods or simulation). This in turn will allow to refine the model (meta model and/or states and dependencies), leading to a continuous improvement of understanding (see Figure 4 for an illustration). This section introduces our suggestions to implement the modeling and reasoning steps of the cycle.

A. Modeling – Introduction of the Meta Model

Starting from the described building blocks we developed a risk model, comprising a model of attack, a model of target of attack and an impact model. These are correlated via well-defined elements of an enterprise architecture model. In this section, we describe the meta models of the sub-models and the correlation method. Figure 5 shows a simplified visualization of the current version of the meta model.

The attack model comprises the category *Actor* which describes the known or assumed potential threatening entities, their type (e.g. state actor or hacktivist) and their related motivation. The category *resources* describes financial resources of the actor, sophistication (know-how), number of personnel, infrastructure, attack tools and malware with appropriate internal and external dependencies. The campaign contains the TTP (tactics, techniques and procedures) which are in turn comprised of single actions. The single actions can be sub-structured in different types according to so-called *kill chain* models [32], which e.g. discriminate actions to intrude a system, actions to spread out within the attacked network, to exploit relevant systems and communication channels and finally to perform the actions which lead to the realization of intended effects.

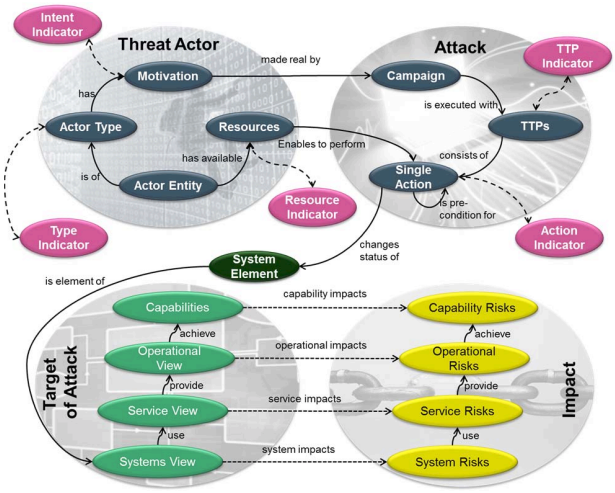

Fig. 5. Cyber Risk Assessment Meta Model

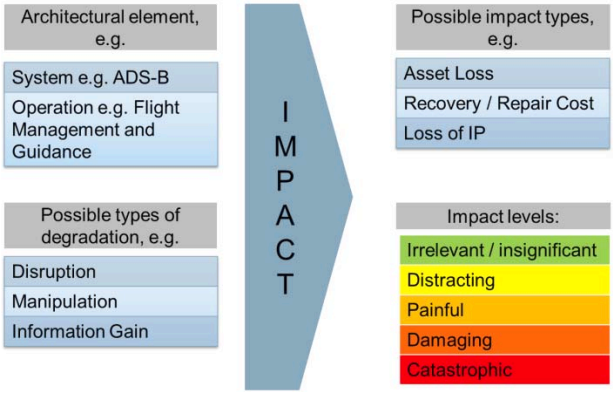

Fig. 6. Impact Model

The meta model of the target of attack is a sub-set of the meta-model of the enterprise architecture. This meta-model describes the elements and dependencies of so-called views of the architecture: The system view again comprises the elements of the ATM system which might be attacked and serves in this way as an interface between the model of attack and the model of the target of attack. The degradations resulting from an attack of these elements are propagated through the architecture using the relations of the architecture model.

Finally the impact model is defined by relating every element of the selected sub-set of the architecture model with pre-assessed impacts (under the assumption of a specific degradation of this element).

B. Modeling – Example of Specific ATM Model

In a specific problem area, a domain model has to be configured according to the structure defined in the meta model. For every node the specific states (or instances) relevant for the application have to be determined. For every pre-defined dependency between nodes, the dependencies of the corresponding states have to be defined according to the meta model.

We explain this configuration process for the ATM example using a specific scenario *ATM capacity degradation* which has been developed for demonstration purposes. It models the risk of potential degradation of the ATM network capacity caused by cyber attacks. For the demonstration we selected a show-case called *ATM capacity degradation by interference with availability and integrity of flight plan information* (see Section IV-A for more details on the scenario).

For this scenario, all possible actors, resources, campaigns and systems, which might cause ATM capacity degradation have to be represented as elements of the attack model. Additionally the usual *noise* caused by various users must be represented as well. The elements of the nodes which are related according to the meta model must be weighted (e.g., it must be defined whether a hacker is motivated to steal information protected by intellectual property rights).

The configuration of the model of target of attack is straightforward. If an architecture model is available we re-use the enumerations and relations of this model. In our case we exploited the data of the EATMA. However, the quality and level of detail of the EATMA are not consistent for all the nodes we need to employ. Therefore, we needed to tune some of the data to get a model fit for demonstration purposes. Note that this effect must be expected for most existing enterprise architecture models because they are usually designed for specific purposes, resulting in sub-models with varying quality.

To complete the overall risk model, the impact model has to be configured. We defined the impact individually for the architecture model elements, as illustrated in Figure 6. This results in a large table which represents the configuration of the impact as defined by experts. Again the approach is designed to integrate as many individual experts as possible to get the best possible assessments for the impact on the different levels of the architecture.

Finally, the actions of the show-case are modeled as events in time. For that reason we considered a specific actor which we assumed to be (with high probability) of a specific type and having the motivation *Degradation of ATM capacity*. For this he might select appropriate TTPs and action chains (e.g., manipulation of flight plan data in information systems or communication channels using suitable malware). If successful this could lead to significant degradations in the operations which are dependent on flight plans and to the associated impacts on the capability or business level.

At the end we have some hundred states within the different nodes of the attack model and the model of target of attack and the corresponding number of dependencies. Therefore, the model represents millions of possible threats. The approach is designed to support domain experts (cyber and ATM experts) to enter and store their data definitions. The approach allows

defining the data node by node so that different types of experts can be integrated into the configuration process. Note here that our configuration of the model of attack serves only as an example which shall be sufficient for the demonstration of the approach.

C. Reasoning

If all models are defined, the reasoning process for the generation of the situational picture comprises three steps:

(i) Use Bayesian networks for calculations within the threat model.
(ii) Propagate results at system level within the EA using relations of the architecture model.
(iii) Calculate risks for the elements with degradation based on pre-defined impacts.

The reasoning within the threat model will be performed using the automatic generation of the BN, reasoning within the BN using COTS software and back-translation of the results to the threat model. The reasoning can be performed using the BN methodology, the results are back-translated to and represented within the user model. If the results within the attack model are approved by threat experts, they are used to generate results concerning the degradation of the elements of the target of attack model by starting with the results at system level and propagating them using the relations of the architecture model. If these results are approved the risk situation can be calculated for the degraded elements of the architecture using the predefined impact assessment.

D. Automatic Generation of Bayesian Network from User oriented Model

One challenge using BNs for this application is the generation and maintenance of a BN for the Cyber Threat domain as described above in the STIX description. This type of domain model will lead to large BN which cannot be handled manually. Additionally even well-educated humans have problems handling statistical information formally, especially conditional probabilities [33]. Therefore we used a method which generates the BN automatically from the attack model [34] as described above, which has a complexity and a formal representation that can be handled by domain experts.

IV. Practical Evaluation and Application

Our model-based approach can be used for various applications in the area of risk assessment, both on strategic and operative-technical level. The objective of our current work is to show the feasibility of the approach and to get exemplary results which can be used for the improvement of resilience against cyber threats in the ATM domain. Due to the ongoing nature of our research work, current results are only preliminary. We are continuously evolving the threat model as well as the model of target of attack. This also includes iterative changes of the attack meta model and the enterprise architecture model. The development of the meta model requires the availability of experts for Bayesian Networks to avoid models which lead to inefficient BNs. It is also important to avoid the combinatorial explosion of necessary impact assessment by selecting an appropriate level of detail. To develop the model for an operational system, there is a need to have interdisciplinary expertise which includes threat intelligence experts, cyber experts on the system level and architectural experts. This section proceeds with an introduction of the basic scenario that was used to guide demonstrator development followed by an overview of the envisaged applications of our approach and closes with a summary of the development status of our prototype.

A. Basic Scenario

For the demonstration of our approach within the scenario *ATM capacity degradation by interference with availability and integrity of flight plan information* we analyzed the systems and data flows for flight plan generation and exchange.

Figure 7 shows the different systems and information exchanges which are possible targets of attack (information taken from Cook [35]). Based on this analysis we derived several manipulation examples (see Figure 8). Our intention is to define attacks which can be applied inconspicuously so that an attacker can remain undetected for long periods of time.

A cyber attack is performed to intrude the described systems. After installation of the appropriate malware at the target systems, he is able to direct various manipulation functions. The aim is to generate significant degradation effects while hiding the malicious nature of their origin. If a user recognizes a specific manipulation, the attacker is able to change the type of manipulation to remain undetected. In manipulation example 3 (*change of restrictions in the route availability document (RAD)*), the allowed flight level of a specific important route might be changed (e.g., from FL 330 to FL 230, which could also have been caused by human error, as well). In consequence, flight plans will be generated according to this restriction, leading to inefficient routes and an overload of lower sectors. In manipulation example 7, an invalid route point might be inserted into a flight plan delivered to the aircraft, resulting in inconsistencies between the flight plan used by the pilot of an aircraft and the flight plan of the ATM operator. Currently we are analyzing and discussing the described manipulation examples with experts to elaborate applications of those examples, which are realistic and lead to the desired degradation effects. These examples are used to define a list of potential attacks as basis of demonstrations.

B. Envisaged Applications

The main areas of application of our model-based approach, that we envisage at the current time, are in the areas of (i) risk assessment and analysis for resilient system design and (ii) dynamic risk management as part of security management operations.

A major challenge in many system development or improvement programs is to design security measures and processes into the systems from the beginning. We foresee the use of our approach for a holistic risk assessment that can already be employed in requirements capturing and system design

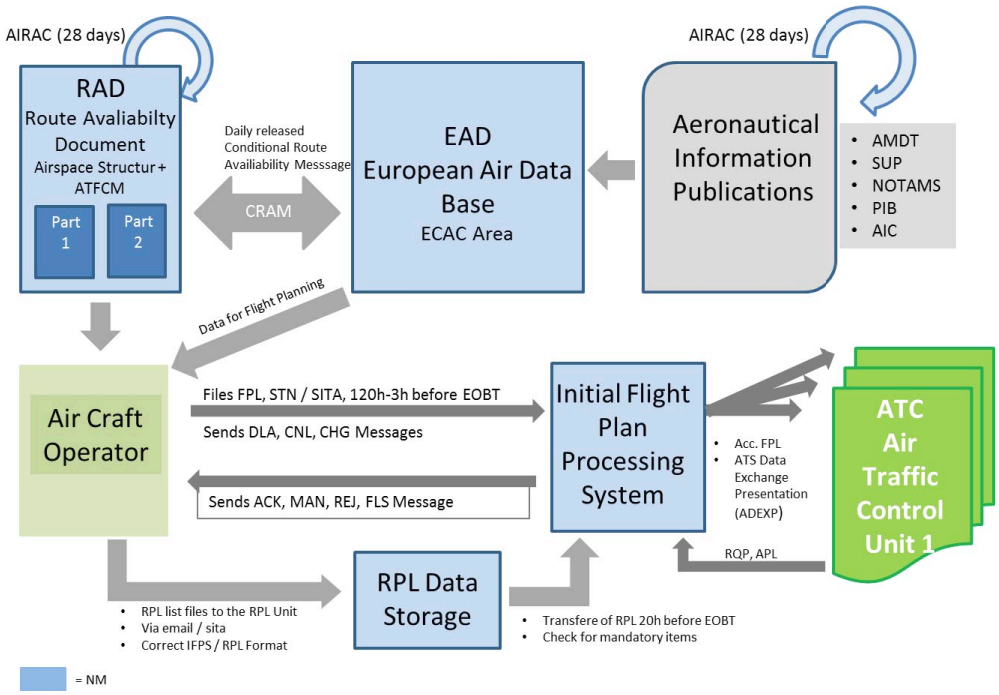

Fig. 7. Flight Plan Data Flow

phases (application (i) above). Depending on the amount of data available at a specific point in time in the system engineering process, more or less abstract risk models can be specified and used for risk analysis as basis for a capture and thorough analysis of security requirements consistent to other functional and non-functional requirements. With this approach, various system design options can be assessed against identified security requirements in a very early phase, reducing the costs and increasing the efficiency of security measures. Additionally, this allows for the design of cyber-resilient processes and systems. A general assumption for the use of our tool in this area is that the risk model is of a more abstract nature, focusing on processes and system functions rather than specific technical systems.

In application area (i), our approach would be typically employed in a project context as part of a system engineering program. In contrast to this, application area (ii) is concerned with actual operation of a system, or more specifically the operation of security management processes as part of overall system operations. Here, we envisage the use of our approach and tool for dynamic risk management, where the tool is aimed at supporting the situational awareness about relevant cyber risks and threats to the system in operation. The functionality of the tool is aimed at the provision of risk and threat-oriented situational pictures besides interactive analysis capabilities.

More details on the potential applications and the specific functionality of our tool in these contexts will be provided in future publications.

C. Prototype Development

We are currently in the act of implementing a prototype to demonstrate the core functionality of this application. The most important use cases for this prototype are shown in Figure 9. We prioritized the functionality which primarily supports the use cases *Model Definition and Maintenance*, *Generation and Analysis of Situational Picture*, *Course of Action Analysis* and *Indicator Detection*.

The demonstrator will have the following functionalities: digital representation of the three sub-models; definition and change of the meta-models if required including the dependencies between the elements of the meta-model; definition of the states of all elements of the nodes as defined in the meta model; definition of the weights of the dependencies between the states; implementation of the BN generation from the attack model as well as the reasoning within the BN and the visualization of the results within the user model; support of analysis within the user model; generation of situational pictures taking into account all indicators which are available at the time where the picture is generated; support of the reasoning within the model of target of attack based on the EATMA relations represented in the meta-model; and support of the calculation of impacts based on the pre-defined expert assessments as described above.

Note that the demonstrator allows to change the meta models and the states of the model continuously. This is a necessity to be able to always represent the current state of knowledge about the domain.

Szenario	Target	Action on Target	PrePl	Flight
1	RAD	Faked opening / closure of conditional routes in the "xyz area"	✔	✔
2	RAD	Faked distribution of route flow restriction for different FPL's	✔	
3	RAD	Change of RAD restrictions	✔	
4	AIP / EAD	Distribution of invalid Pre – Flight Information Bulletin (PIB) Message " Aerodrome XYZ closed due to emergency in progress"	✔	✔
5	IFPS	Invalid REJ or FLS Message of FPL to A/C Operator	✔	
6	IFPS	Invalid cancellation of FPL Data at EOBT -10min	✔	
7	IFPS ATC	Manipulation of FPL Data Route / Speed	✔	✔
8	ATC	Manipulation of Aircraft Type and Wake Category		✔
9	RPL	Revision of RPL NLST or RLST from different A/C Operator at EOBT - 21h	✔	
10	CASA ETFMS	Distribution of invalid Slot Allocation Message for different FPL`s	✔	

Fig. 8. Examples for Manipulations of Flight Plan Related Data

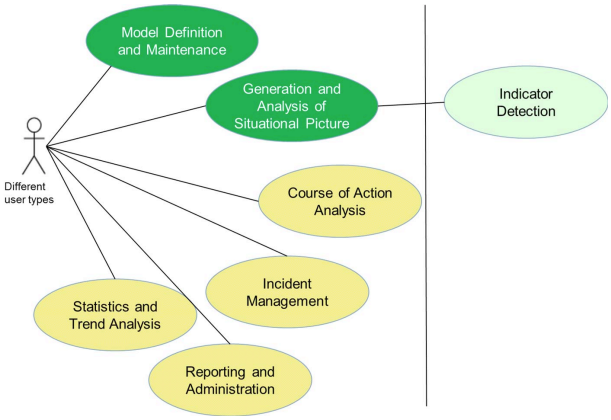

Fig. 9. Use Cases for Dynamic Situational Analysis Demonstrator

V. Conclusions and Future Work

Cyber security risk management is a major challenge in the aviation domain due to the complexity of interconnected infrastructures as well as the uncertainty and high rate of change inherent in cyber-threat related information. To cope with these challenges, we propose the adoption of a model-based approach to enable holistic understanding of cyber-threat related risk in aviation. Our approach comprises modeling and analysis steps. Our suggestion is to use a combination of existing enterprise architecture, threat and impact modeling approaches resulting in a unified holistic risk meta-model. We use specific instances of this meta model with a partial translation into Bayesian Networks for computer-assisted analysis on a system of systems level. A demonstrator of a dynamic risk management application based on this approach is currently being implemented. Preliminary results from the demonstrator show promising results.

A major objective of our approach is its efficiency due to the re-use of approved structures, elements and data. This allows for the creation of big risk models with reasonable effort. The approach is sustainable due to the re-use of building blocks of enterprise architecture models and STIX threat models, which are already standardized or will be standardized in the near future. Finally we believe to have a modern and solid approach for reasoning within the model using the inherent functionality and power of Bayesian Networks, i.e., causal analysis (what-if-analysis), reasoning based on current evidence (for situational awareness analysis), automatic detection of contradictory evidence and explanation of results.

A challenge inherent in our approach is to bring together the necessary domain expertise. This is essential for the definition of models which are consistent concerning the level of detail and value of data in the various nodes. On the other hand this necessity provides a good opportunity to integrate the knowledge of multiple experts into one overall model supporting the analysis and understanding of different types of users. To support the structured cooperation of experts in this context, suitable processes have to be implemented. Another challenge is to approve the quality and consistency of the enterprise architecture model. The size of BN which can be calculated within a reasonable time may be a future challenge but we expect that the power of computers used in real applications should be sufficient.

An additional promising future work is to create interfaces of the risk model to simulation models, which are available for the ATM domain to complement the reasoning within the risk model.

The main challenge for a real-life application of the dynamic risk management application is the generation and continuous maintenance of data in all sub-models. On the technical side, this calls for an increased use of automation, which shall comprise (i) a semi-automatic read-in of elements of attack models using the growing possibilities of STIX, and its data exchange TAXII (Trusted Automated eXchange of Indicator Information [36]) and (ii) a semi-automatic configuration of target of attack model using the XMI-format which is the standard format for the exchange of enterprise architecture models [37]. However, first and foremost, this is an organizational issue, as the support and cooperation of multiple stakeholders is needed to get comprehensive access to the relevant data. Main future research will be focused on a thorough experimentation of our approach based on real data. This will also serve to enlighten some of the essential open questions in the context of our approach: the appropriate level of complexity and detail in the risk model.

Acknowledgment

This paper presents some of the results of the ARIEL (Air Traffic Resilience) project supported by the Bavarian State Ministry of Economics, Media, Energy, and Technology as part of the Bavarian Aviation Research Program. We would like to thank the partners of the ARIEL project for their general support in the work that led to this paper. Special thanks also go to the anonymous peer reviewers for their encouragement and constructive feedback.

REFERENCES

[1] R. Kölle, G. Markarian, and A. Tarter, *Aviation Security Engineering: A Holistic Approach*, ser. Artech House intelligence and information operations series. Artech House, 2011.

[2] "Hackers Target Polish Airline LOT, Ground 1,400 Passengers," http://bit.ly/1daLI9X.

[3] "All U.S. United Flights Grounded Over Mysterious Problem," http://bit.ly/1dJmmRK.

[4] T. Vaudrey, "European ATM Architecture," available at http://bit.ly/1Rox14J.

[5] S. Barnum, "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)," *MITRE Corporation*, vol. 11, 2012.

[6] "Enterprise Architecture," https://en.wikipedia.org/wiki/Enterprise_architecture.

[7] "SESAR eATM Portal," https://www.atmmasterplan.eu/architecture/home.

[8] I. C. A. Organization, Ed., *ICAO Doc 9750 – 2013–2028 Global Air Navigation Plan*, fourth edition ed. Montreal: ICAO, 2013.

[9] "Working Document for the Aviation System Block Upgrades," bit.ly/21kIh57, 2013.

[10] "NATO Architecture Framework Version 3.1," http://www.nhqc3s.nato.int/ARCHITECTURE/_docs/NAF_v3/ANNEX1.pdf.

[11] P. Ravenhill and M. Shreeve, "SESAR Strategy and Management Framework Study for Information Cyber-Security," SESAR JU, Tech. Rep., 2015, http://bit.ly/1L5wT9d.

[12] I. C. A. Organization, Ed., *Annex 17: Security – Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, amendment 14 ed. Montreal: ICAO, 2014.

[13] BSI, *IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik*. Bundesdruckerei, 1992.

[14] "Commission Implementing Regulation (EU) No 1035/2011 of 17 October 2011," http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1035&from=EN.

[15] S. JU, "SESAR ATM Security Risk Assessment Methodology – Deliverable 16.02.03; SESAR WP16.2-ATM Security."

[16] "EUROCAE WG-72 – Aeronautical Information Systems Security," https://www.eurocae.net/wgs/active/?wg=WG-72.

[17] "RTCA SC-216 – Aeronautical Systems Security," http://www.rtca.org/content.asp?pl=108&sl=33&contentid=82.

[18] "EN 16495:2014 – Air Traffic Management – Information security for organisations supporting civil aviation operations."

[19] "Structured Threat Information eXpression (STIX) – A structured language for cyber threat intelligence," http://stixproject.github.io/.

[20] "STIX idioms," http://stixproject.github.io/documentation/idioms.

[21] J. Pearl, *Probabilistic reasoning in intelligent systems: networks of plausible inference*. Morgan Kaufmann, 2014.

[22] N. Fenton and M. Neil, *Risk assessment and decision analysis with Bayesian networks*. CRC Press, 2012.

[23] G. C. Oatley and B. W. Ewart, "Crimes analysis software:'pins in maps', clustering and Bayes net prediction," *Expert Systems with Applications*, vol. 25, no. 4, pp. 569–588, 2003.

[24] R. Boondao, V. Esichaikul, and N. K. Tripathi, "A Bayesian network model for analysis of the factors affecting crime risk," *WSEAS Transactions on Circuits and Systems*, vol. 3, no. 9, pp. 1895–1900, 2004.

[25] D. C. Daniels, L. D. Hudson, K. B. Laskey, S. M. Mahoney, B. S. Ware, and E. J. Wright, "Terrorism risk management," *Bayesian Networks: A Practical Guide to Applications*, pp. 239–262, 2008.

[26] P. Wijayatunga, S. Mase, and M. Nakamura, "Appraisal of companies with Bayesian networks," *International Journal of Business Intelligence and Data Mining*, vol. 1, no. 3, pp. 329–346, 2006.

[27] E. Ejsing, P. Vastrup, and A. L. Madsen, "Predicting probability of default for large corporates," *Bayesian Networks: A Practical Guide to Applications*, pp. 329–344, 2008.

[28] "Improved decision-support for air traffic management and planning," http://www.agenarisk.com/agenarisk/case_02.shtml.

[29] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using Bayesian networks for cyber security analysis," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*. IEEE, 2010, pp. 211–220.

[30] S. Y. K. Mo, P. A. Beling, and K. G. Crowther, "Quantitative assessment of cyber security risk using Bayesian Network-based model," in *Systems and Information Engineering Design Symposium, 2009. SIEDS'09.* IEEE, 2009, pp. 183–187.

[31] D. Kolev, R. Koelle, R. A. C. Rodriguez, and P. Montefusco, "Security Situation Management - Developing Concepts of Operations and Threat Prediction Capability," in *Digital Avionics Conference 2015*, 2015.

[32] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, p. 80, 2011.

[33] G. Gigerenzer, *Das Einmaleins der Skepsis: über den richtigen Umgang mit Zahlen und Risiken*. eBook Berlin Verlag, 2014.

[34] J. Ziegler and B. Haarmann, "Automatic Generation of Large Causal Bayesian Networks from User Oriented Models," in *Proceedings of the 6th Workshop on Sensor Data Fusion (INFORMATIK 2011: Informatik schafft Communities)*. Citeseer, 2011.

[35] A. Cook, *European air traffic management: principles, practice, and research*. Ashgate Publishing, Ltd., 2007.

[36] "Trusted Automated eXchange of Indicator Information," https://taxiiproject.github.io/.

[37] "XML Metadata Interchange," http://www.omg.org/spec/XMI/.