Towards Combined Safety and Security Constraints Analysis

Daniel Pereira[1], Celso Hirata[1(✉)], Rodrigo Pagliares[1,2], and Simin Nadjm-Tehrani[3]

[1] Instituto Tecnológico de Aeronáutica, São José dos Campos 12228-900, Brazil
dpatricksp@gmail.com, hirata@ita.br,
pagliares@bcc.unifal-mg.edu.br
[2] Universidade Federal de Alfenas, UNIFAL-MG, Alfenas, MG, Brazil
[3] Linköping University, Linköping 581 83, Sweden
simin.nadjm-tehrani@liu.se

Abstract. A growing threat to the cyber-security of embedded safety-critical systems calls for a new look at the development methods for such systems. One alternative to address security and safety concerns jointly is to use the perspective of modeling using system theory. Systems-Theoretic Process Analysis (STPA) is a new hazard analysis technique based on an accident causality model. NIST SP 800-30 is a well-known framework that has been largely employed to aid in identifying threats event/source and vulnerabilities, determining the effectiveness security control, and evaluating the adverse impact of risks. Safety and security analyses, when performed independently, may generate conflicts of design constraints that result in an inconsistent design. This paper reports a novel integrated approach for safety analysis and security analysis of systems. In our approach, safety analysis is conducted with STPA while security analysis employs NIST SP800-30. It builds on a specification of security and safety constraints and outlines a scheme to automatically analyze and detect conflicts between and pairwise reinforcements of various constraints. Preliminary results show that the approach allows security and safety teams to perform a more efficient analysis.

Keywords: Safety analysis · Security analysis · STPA · NIST SP800-30

1 Introduction

Safety-critical systems are becoming complex with many components reused in integration of subsystems in order to reach a common goal. Cyber-security threats are becoming a growing concern while developing of safety-critical systems [1]. The use of commercial off the shelf software across the aviation, maritime, rail and power-generation infrastructures has resulted in increased number of vulnerabilities. Johnson [1] points out that existing office-based security standards cannot be easily integrated with safety-critical systems standards easily. There is an urgent need to move beyond high-level policies and address the more detailed engineering challenges. This view is supported by the ways in which cyber-security concerns undermine traditional

S. Tonetta et al. (Eds.): SAFECOMP 2017 Workshops, LNCS 10489, pp. 70–80, 2017.
DOI: 10.1007/978-3-319-66284-8_7

forms of safety assessment and the ways in which safety concerns hinder the deployment of conventional mechanisms for cyber-security.

An alternative to address security and safety concerns jointly is to use the perspective of modeling using system theory. STAMP (Systems-Theoretic Accident Model and Processes) [2] is an accident causality model based on system theory. Within STAMP, safety is viewed as a control problem rather than a reliability problem. STAMP is built on top of three basic constructs: safety constraints, hierarchical safety control structures and process models. STAMP, due to its underlying basis - system theory - is a sound model that can be considered to fit not only safety concerns but also security concerns.

STPA (Systems-Theoretic Process Analysis) [3] is a safety analysis technique based on STAMP. STPA allows the identification of several factors contributing to accidents such as software flaws, decision-making errors, hazardous component interactions, and organizational, and management deficiencies. STPA has two steps. The first step identifies the unsafe control actions that can lead to system unsafe behavior. The second step identifies the potential causes of scenarios leading to unsafe control, and thereafter effectively identifying safety requirements.

There are two recent approaches, STPA-Sec [4] and STPA-SafeSec [5], which aid in the joint elicitation of functional, safety, and security requirements. However, both approaches are very recent and lack extensive experience in real case studies. We also believe that techniques and tools to support the requirement engineering of cyber-security of safety-critical systems and more investigations on integration of existing techniques are required.

NIST Special Publication 800-30 [6] is a guide for conducting security risk assessments. It provides guidance for carrying out tasks of a risk assessment process that are preparing for, conducting, communicating the results, and maintaining the assessment. The NIST SP800-30 framework uses six steps to break down its activities. The first two steps are identifying threat events/sources and vulnerabilities. Other steps consist in determining the effectiveness of security control, evaluating the adverse impact of risks as a combination of impact and likelihood. We will consider NIST SP800-30 because many organizations in the United States, particularly those in the aerospace area, align to the standard. Moreover, NIST SP800-30 is a flexible framework that provides a standard report structure. We will focus on the first two steps of NIST SP800-30.

Security concerns are relatively new in domains such as aeronautics and space. Some specific standards to address it have been developed [7]. Currently, security and safety specialists have their own processes enacted by distinct teams. We claim that security and safety teams conducting their analyses rather independently may produce inconsistent designs. The inconsistency is characterized by the existence of conflicting requirements.

Another issue is related to the satisfaction of requirements in an effective manner. *Reinforcement* is characterized by similarity of security and safety requirements, i.e. requirements that can be satisfied by similar (or same) features. We argue that safety and security requirements that have a reinforcement relationship can be addressed jointly in a more effective manner. Therefore, it is useful to have a systematic approach

that aids identifying conflicts and reinforcements between security and safety requirements and addresses them in an integrated manner.

We propose a novel integrated approach for security and safety analyses of systems to analyze both concerns jointly using NIST SP800-30 and STPA. It builds on specifications to define security and safety constraints and drives a scheme to automatically analyze and detect conflicts and reinforcements between security and safety constraints. The idea is that the proposed approach aids security and safety teams to resolve conflicts early during system life cycle (concept phase), and to perform a more efficient analysis.

The remainder of this paper is organized as follows. The related work is presented in Sect. 2. Section 3 introduces our approach. Section 4 presents an example of use of the approach and Sect. 5 concludes the paper.

2 Related Work

Oates et al. present a SysML technique for security and safety using HiP-HOPS (Hierarchically Performed Hazard Origin and Propagation Studies) and SDL (Secure Development Lifecycle) [8]. They assume that there is a significant overlap between security and safety analysis activities. However, it is not clear which are those overlapping activities. They do not deal with conflicts between security and safety.

Subramanian and Zalewski [9] apply a NFR (Non-Functional Requirements) approach to evaluate security and safety properties. The NFR approach uses an ontology, which defines elements such as soft goals and contributions. Security and safety analyses occur together; in the same graph, the security and safety goals are displayed with contributions. Trade-offs between security and safety requirements are handled, but there is no distinction between which activity should be performed by the safety or security team.

Young and Leveson propose an integrated approach to security and safety called STPA-Sec [4]. The approach is based on STAMP [2] and extends STPA [3]. It helps identifying security vulnerabilities, safety hazards, requirements, and scenarios leading to violation of security and safety constraints. As a result, the analysis allows refining system concept by addressing not only technical but also organizational issues. STPA-Sec is a very recent work, with little documentation and history of usage. The approach does not describe how security and safety teams share information with each other in order to detect conflicts between security and safety constraints.

Similar to STPA-Sec, Friedberg et al. [5] present an analysis methodology for both security and safety, called STPA-SafeSec. The core contribution is the description of a generic component layer diagram to evaluate whether security constraints are assured or not. Their work provides a list with the cyber-attacks on integrity and availability at component layer to analyze the malicious effect. The methodology neither mentions the relationship between security and safety constraints nor discriminates the activities performed by security and safety teams.

Nostro et al. [10] describe a general methodology to support the assessment of safety-critical systems with respect to security aspects. The methodology defines a security threat library based on NIST SP800-53 (Security Controls). It is not clear in

their methodology how the security and safety assessments are jointly performed. The authors state that there may be conflicts between security and safety concerns but they do not describe how to resolve them.

Thomas [11] presents a model-based technique to automate conflict detection between safety requirements and other functional requirements during early development of a system using the results of a hazard analysis. A conflict is defined when it is hazardous for the controller to provide and at the same time not to provide a control action. This approach neither considers security constraints nor takes into account reinforcements of constraints.

Troubitsyna [12] describes briefly a structured integrated derivation of safety and security requirements from safety goals. It relies on a widely accepted safety case technique and enables the integrated treatment of safety and security; however, conflicts are not dealt with.

Katta et al. [13] present an approach for providing traceability to an assessment method to combined harm of safety and security for information systems. Their goal is to capture the interdependencies between the safety and security requirements and to demonstrate the history and rationale behind their elicitation. Their approach does not deal with conflicts between safety and security constraints.

Netkachova et al. [14] present an approach to conduct structured safety and security analyses. Their approach creates safety cases that provide safety justification taking into consideration security issues. The approach is applied to a gateway function based on Multiple Independent Level of Security (MILS). The defined integrated policy considers safety and security domains and resolution of conflicts. However, the authors do not present how conflicts are identified and resolved. There is no information about which activity should be performed by the safety or security team respectively.

Many works investigate the relationships between NFR (Non-Functional Requirements) [15–19] using different strategies such as ontology, graph, model table, and taxonomy. There is a consensus that early identification of conflicting requirements is an important task during system development. However, most of the works [15–19] provide means to identify requirement conflicts only in the development phase of system's lifecycle. Few investigations are concerned with correlation or reinforcement of requirements. Egyed and Grunbacher [15] recognize the need to identify requirements conflict and cooperation, which is similar to our *reinforcement*. They consider requirement correlation during the analysis of conflict. Only Hu et al. [17] consider semantic modeling to identify requirement conflicts. Our proposed approach differs from the related work in the sense that detection of conflicts and reinforcements takes place during safety and security analyses at an earlier stage (concept phase). Besides, our detection is automatically performed using a specification of security and safety constraints.

3 Proposed Approach

Our approach builds on a process that allows interaction between both teams in specific stages of analysis. The interaction happens more deeply when the teams identify relationships between security and safety concerns. We claim that the joint analysis is

made easier if we use constraints instead of requirements. The idea is to verify whether the satisfaction of a safety constraint affects a security constraint, and vice-versa. As indicated, the relationship between satisfaction of security and safety constraints can be a conflict or a reinforcement. When the sets of security and safety constraints do not conflict, a design that satisfies both sets is consistent (considering the current environment).

The proposed approach consists of a workflow of activities depicted in Fig. 1. We group the activities into three sets: safety, security, and integration. In Fig. 1, safety activities are depicted in the upper part while the security activities are shown in the lower part. Activities shared by security and safety teams are exhibited between the two parts.

STPA and NIST SP800-30 are safety and security techniques, which are based on systems engineering and should be deployed early in the system life cycle. Security and safety specialists usually perform their analysis independently, generating their own security and safety requirements from security and safety constraints.

With respect to the integration set, the activities require expertise of both teams: security and safety. It also requires the expertise of systems theory, to provide a theoretical foundation for the approach. The integration set includes two activities: "Define System Goals and its Context", and "Perform Integrated Analysis". The first one is related to the technical foundations and assumptions while the second activity is about performing a joint analysis of security and safety.

Before both teams begin their own analysis, a joint meeting is required. The activity "Define System Goals and its Context" establishes a context for the security and safety assessment according to stakeholder needs. This context includes identifying the purpose and scope of the assessment and identifying unacceptable losses, assumptions and constraints associated with the assessment, system boundaries, and other relevant information to perform the security and safety assessment. Once the system foundation is established, both teams can follow their own processes and discuss the security and safety constraints.

"Perform Integrated Analysis" is an activity where security and safety teams work together to identify conflicts between security and safety constraints and jointly define security measures and safety recommendations (SMSR). The inputs are the security and safety constraints and the outputs are the relationship between the security and safety constraints and the defined SMSR for each security and safety constraint, which are recorded in a document called "Security and Safety Dossier". The activity is divided into four tasks, not shown in Fig. 1: "Analyze the relationships between security and safety constraints", "Resolve conflicts", "Define security measures and safety recommendations", and "Elaborate security and safety dossier". In the example in Sect. 4, we will detail the tasks. The activities "Identify Causal Factors and Scenarios", "Determine Security Control, Adverse Impact and Risk", and "Maintaining and Monitoring Risks" are activities that security and safety teams can perform more independently. More information about these activities can be obtained elsewhere [3, 6].

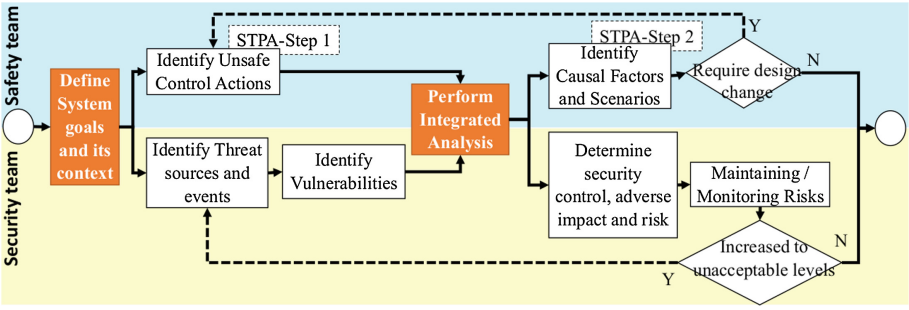

Fig. 1. The proposed integrated approach

4 Example of Use

In order to illustrate the use of our approach, we consider a simple example of a revolving door system (RDS). Figure 2 illustrates the main components of the system: (i) a revolving door that has a controller with an embedded software with a metal detection function, and a receptor device to receive commands from the remote-controller, (ii) a repository for personal belongings (including metals) and (iii) a security guard (SG) with a remote-control device. The maintenance team (not shown in the figure) can configure the metal detector's sensitivity. The SG can lock or unlock the system through a remote control or a key. The revolving door detects metal objects (e.g. gun) through the embedded software. The repository for personal belongings allows customers/employees to put their personal belongings for SG inspection. The system is used in banks and other types of office facilities. Usually there is only one door system per office facility.

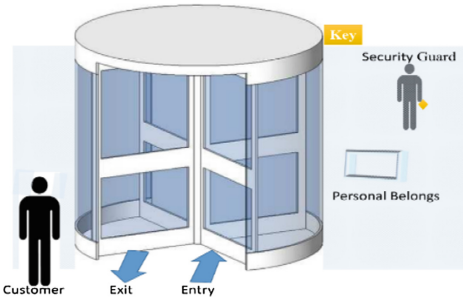

Fig. 2. Revolving door system (RDS)

For the activity "Define system goals and its context", two accidents are identified: (i) people killed or injured and (ii) damage to facility. The following hazards are identified: (i) armed and unauthorized person inside the bank branch, (ii) revolving

door unlocked, (iii) disruption of power supply, and (iv) revolving door locked during an emergency. The control structure for the RDS elaborated has five components: security guard, person, RDS controller, and electrical system controllers, and controlled process. Responsibilities, process model, and mental model are identified for each controller.

In the activity "Identify Unsafe Control Actions", unsafe control actions are identified for each controller. For RDS, twelve unsafe control actions are identified and twelve safety constraints are derived. Table 1 illustrates some unsafe control actions and safety constraints of RDS. An example of identified unsafe control is when there is an emergency (triggered by external information such as fire alarm), the RDS controller has to issue unlock door command but it fails to do so (UCA-5.1). In this situation, people can be held locked in the building during a fire. The safety constraints (SaCs) are directly derived from the unsafe control actions. For instance, for the above unsafe control action, the corresponding safety constraint is "RDS must provide unlock door command when there is an emergency".

Table 1. Some unsafe control actions and safety constraints identified for RDS

Unsafe control action	Safety constraint
UCA-5.1: RDS does not provide unlock door command when there is an emergency	SaC-5.1: RDS must provide unlock door command when there is an emergency
UCA-5.2: RDS provides unlock door command when an armed person is in the entrance lane	SaC-5.2: RDS must never provide unlock door command when an armed person is in the entrance lane
UCA-6.1: RDS provides lock door command when there is an emergency	SaC-6.1: RDS must never provide lock door command when there is an emergency

In the activities "Identify Threat Sources and Events" and "Identify Vulnerabilities", two sources of threats are identified: (i) human, and (ii) environmental and physical. Seven threats are identified from these sources, which result in nine vulnerabilities. Table 2 illustrates some vulnerabilities and security constraints (SeCs). An example of vulnerability is "Unlocked revolving door during an emergency". Ten security constraints are derived from the vulnerabilities. The security constraint corresponding to the aforementioned vulnerability is "RDS must never unlock the revolving door during an emergency".

The "Perform Integrated Analysis" activity consists of four tasks as presented in Fig. 3:

The goal of the task "Analyze the relationships between security and safety constraints" is to identify the type of relationship between security constraints and safety constraints. The identification is based on the type of influence that satisfaction of one constraint has on another constraint. The influence may be positive (reinforcement) or negative (conflict).

Table 2. Some vulnerabilities and security constraints identified for RDS

Vulnerability	Security constraint
Vul-06: Incorrect parameters set up (e.g. metal detector's sensitivity)	SeC-06.1: The maintenance team must set up RDS with the correct parameters
	SeC-06.2: The maintenance team, only when authorized, must configure RDS
Vul-07: Lack of redundancy for critical activities	SeC-07: RDS must provide redundancy in critical activities
Vul-08: Lack of power supply generation	SeC-08: Electrical System must never be interrupted when the system is operating
Vul-09: Unlocked revolving door during an emergency	SeC-09: RDS must never unlock the revolving door during an emergency

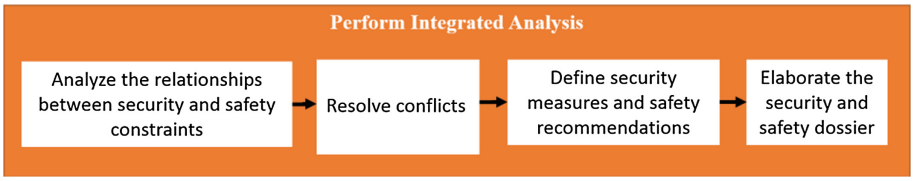

Fig. 3. Perform integrated analysis process

To identify the relationship, we employ the tokenization of safety constraint specifications proposed by Thomas [11]. The specification is expressed as four-tuple: (i) source controller that can issue control actions, (ii) type of control action (*must provide* or *must not provide*), (iii) control action, and (iv) context in which the control action must or must not be provided.

Similarly, we propose to use the tokenization for security constraint specifications with four-tuple: (i) agent that has the capability to perform an action in the asset, (ii) type of action taken by the agent (*must provide* and *must not provide*), (iii) action taken by the agent, and (iv) system and assets state when the action must or must not be provided. With the specifications, we derive an automatic scheme to detect conflicts and reinforcements.

We analyze the relationships between twelve safety constraints (SaC) and ten security constraints (SeC) using the scheme. For instance, the scheme automatically detected the conflict between the SeC "RDS must never unlock revolving door during an emergency" and SaC "SG must manually/remotely provide unlock door command during an emergency".

We suggest two alternatives to resolve conflicts. The first alternative is to redefine the components, processes, and operations of the system, so that the new constraints do not conflict. The second alternative is to refine the constraints. The idea is to take into consideration the identified conflict and refine the constraint in space and/or time to define more refined constraints that do not conflict with each other. We call the first alternative as "system redefinition" and the second, "constraint refinement". We used the second alternative for the conflict we identified earlier.

Most of the times, it is difficult to discern which emergency is going on: just security, just safety, or both. Based on that, both constraints should be redefined using the two independent lanes of the RDS to meet all types of emergency. Thus, the safety constraint should be detailed by using two independent lanes: exit and entry. During an emergency, the entry lane must be blocked and the exit lane must be controlled. Considering the decomposition, the security and safety constraints should be rewritten as follow: "SG must manually/remotely provide unlock door command for exit lane during an emergency" and "RDS must never unlock revolving door for entry lane during an emergency". The constraints do not conflict with each other any longer because there are two separate lanes.

In the task "Define security measures and safety recommendations", the security and safety teams identify and analyze the SMSR that best satisfy the security and safety constraints. In our example, in order to provide a physical implementation for the two lanes, we consider two independent doors - one for entry and other for exit – as a recommendation. Following this change in design, the analysts should state whether each constraint (security and safety) is complete or partially addressed. After identifying reinforcement relationships, the safety and security analysts should work together in the task of defining SMSR. It is expected that the resulting SMSR will be more effective.

The "Elaborate security and safety dossier" task documents the security and safety constraints and their relationships during security and safety assessments. It also documents the security measures, safety recommendations and system vulnerabilities. The security and safety dossier ensures that all identified constraints were addressed as expected by the safety and security teams through the SMSR. Verification (testing) is not covered here; however, once the SMSR are implemented, the verification activities shall be performed to check the security and safety effectiveness.

5 Concluding Remarks

We propose an integrated approach for the analysis of security and safety risks with automatic detection of conflicts and reinforcements. The joint analysis of security and safety constraints within different teams aligns with current safety and security best practice processes (STPA and NIST SP800-30 respectively). We simply augment the approaches with automatic detection of conflicts and their resolution, or identified reinforcements that may be useful in a later risk quantification and mitigation activity.

In a current work, we are applying the proposed approach in a larger and more complex system. The system is the Flight Management System (FMS). FMS is a specialized computer system that automates a wide variety of in-flight tasks, reducing the workload on the flight crew. Preliminary results [20] have shown that it is practically unfeasible to make the integrated analysis manually. We are developing a set of tools to support the analysis, including the tool for automatic detection of conflicts and reinforcements presented in this work.

Acknowledgements. The work of the last author was supported by the national projects on aeronautics (NFFP6-00917) and the research centre on Resilient Information and Control Systems (www.rics.se). The work of the second author was supported by the Conselho Nacional de Desenvolvimento Científico e Tecnológico under grant number Universal 01/2016 403921/2016-3.

References

1. Johnson C.: Why we cannot (yet) ensure the cyber-security of safety-critical systems. http://eprints.gla.ac.uk/130822/1/130822.pdf. Accessed 2017/05/14
2. Leveson, N.: Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, Cambridge (2011)
3. Leveson, N.: An STPA Primer:What is STPA? http://sunnyday.mit.edu/STPA-Primer-v0.pdf. Accessed 12 May 2017
4. Young, W., Leveson, N.: An integrated approach to safety and security based on systems theory. Commun. ACM **57**(2), 31–35 (2014)
5. Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., Sezer, S.: STPA-SafeSec: safety and security analysis for cyber-physical systems. J. Inf. Secur. Appl. **34**, 183–196 (2016)
6. National Institute of Standards and Technology: NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments (2012)
7. RTCA DO-326A: Airworthiness security process specification. RTCA (2014)
8. Oates, R., Foulkes, D., Herries, G., Banham, D.: Practical extensions of safety critical engineering processes for securing industrial control systems. In: 8th IET International System Safety Conference incorporating the Cyber Security Conference Proceedings, pp. 1–6. IET, Cardiff (2013)
9. Subramanian, N., Zalewski, J.: Quantitative assessment of safety and security of system architectures for cyberphysical systems using the NFR approach. IEEE Syst. J. **10**(2), 397–409 (2016)
10. Nostro, N., Bondavalli, A., Silva, N.: Adding security concerns to safety critical certification. In: IEEE International Symposium on Software Reliability Engineering Workshops Proceedings, Naples (2014)
11. Thomas, J.: Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis. MIT Ph.D. dissertation, Cambridge (2013)
12. Troubitsyna, E.: An integrated approach to deriving safety and security requirements from safety cases. In: IEEE 40th Annual Computer Software and Applications Conference Proceedings, Atlanta (2016)
13. Katta, V., Raspotnig, C., Karpati, P., Stålhane, T.: Requirements management in a combined process for safety and security assessments. In: International Conference on Availability, Reliability and Security, Regensburg (2013)
14. Netkachova, K., Müller, K., Paulitsch, M., Bloomfield, R.: Security-informed safety case approach to analysing MILS systems. In: International Workshop on MILS: Architecture and Assurance for Secure Systems, Amsterdam (2015)
15. Egyed, A., Grunbacher, P.: Identifying requirements conflicts and cooperation: how quality attributes and automated traceability can help. IEEE Softw. **21**(6), 50–58 (2004)
16. Tabassum, M., Siddik, M., Shoyaib, M., Khaled, S.: Determining interdependency among non-functional requirements to reduce conflict. In: International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka (2014)

17. Hu, H., Ma, Q., Zhang, T., Tan, Y., Xiang, H., Fu, C., Feng, Y.: Semantic modelling and automated reasoning of non-functional requirement conflicts in the context of softgoal interdependencies. IET Softw. **9**(6), 145–156 (2015)
18. Sadana, V., Liu, X.: Analysis of conflicts among non-functional requirements using integrated analysis of functional and non-functional requirements. In: 31st Annual International Computer Software and Applications Conference Proceedings, Beijing (2007)
19. Salado, A., Nilchiani, R.: The concept of order of conflict in requirements engineering. IEEE Syst. J. **10**(1), 25–35 (2016)
20. Pereira, D., Hirata, C., Pagliares, R., De Lemos, F.: STPA-Sec for security of flight management system. In: 2017 STAMP Workshop (2017). http://psas.scripts.mit.edu/home/2017-stamp-presentations/. Accessed 12 May 2017