Improving Security and Safety Co-analysis of STPA

Erik Nilsen Torkildson

Wise Consulting, Molde, Norway E-mail: ent@wise.no

Jingyue Li

Department of Computer Science, Norwegian University of Science and Technology, Norway, E-mail: jingyue.li@ntnu.no

Stig Ole Johnsen

SINTEF Digital, Norway, E-mail: Stig.O.Johnsen@sintef.no

Many safety and security co-analysis methods have been proposed to assure the safety of critical systems, including autonomous systems. One example of safety and security co-analysis approach is Systems-Theoretic Process Analysis (STPA) plus STPA-Sec. When using STPA combined with STPA-Sec, the security analysis is performed as part of the causal factor analysis, which is after the safety risk analysis. Few studies have questioned whether such an approach can be improved and how to improve it. In our study, we tried to answer two research questions (RQs): RQ1) Could we improve STPA-Sec by complementing it with threat modeling approaches? RQ2) Could we find more safety risks if we perform security analysis before safety analysis? We performed safety and security co-analysis of an autonomous boat to answer these research questions. Results of the study show that performing security analysis before safety analysis identifies more safety risks than the other way around. To be combined with STPA-Sec, threat modeling based on the data flow diagram outperforms other threat modeling approaches we evaluated.

Keywords: Cyber Security, Safety, Threat Modelling, Autonomous Systems, STPA

1. Introduction

Without systematic security analysis of autonomous systems, hackers may hijack and control the autonomous systems remotely, and creates mishaps. In 2015, Fiat Chrysler Automobiles ordered a recall of 1.4 million vehicles that were vulnerable to a threat of remote control and hijacking (Guzman, 2015). In 2013, Samy Kamkar demonstrated with the Parrot AR that it was possible to hijack drones, with what he called SkyJack (Kamkar, 2013).

As security breaches can bring risks to system safety, many methods have been proposed to consolidate the security and safety co-analysis. Surveys of security and safety co-analysis methods can be found in (Chockalingam, 2016) and (Kriaa et al., 2015). One method to combine safety and security analysis is STPA (System-Theoretic Process Analysis) (Thomas, 2013, Leveson, 2012) combined with STPA-Sec (Young and Leveson, 2013, Young and Leveson, 2014). STPA-Sec extends STPA, which is a safety analysis method. The extension is to include security analysis. STPA-Sec "*Shifts the focus of the security analysis away from threats as the proximate cause of losses and focuses instead on the broader system structure that allowed the system to enter a vulnerable system state that the threat exploits to produce the disruption leading to the loss (Young and Leveson, 2013).*" The security analysis of STPA-Sec focuses on identifying security vulnerabilities that may lead to Unsafe Control Actions (UCAs).

We have performed a study to use STPA and STPA-Sec to analyze safety and security risks of an autonomous boat (Torkildson et al., 2018). We found that the strength of STPA plus STPA-Sec is that it focuses more on safety–security interactions. However, the limitation of the STPA-Sec is that the security analysis focuses mainly on vulnerability that can be the causal factors for safety hazards. The security vulnerabilities, which may lead to information leakage or privacy issues, but will not lead to safety hazards, may be overlooked. Thus, we believe that integrating STPA-Sec with more security-oriented analysis methods, e.g., threat modeling approaches, can be beneficial. In addition, we believe that starting with STPA-Sec and then STPA may help reveal more safety risks. Having these two questions in mind, in this study, we analyzed which threat modeling approach is best to be combined with STPA-Sec for security analysis and whether starting with security analysis can reveal more safety risks. Results of the study show that threat modeling using data flow diagram is better to be combined with STPA-Sec than other threat modeling approaches, such

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2019-paper

as misuse case, attack trees, Business Process Modelling Notation (BPMN), and Socio-Technical Security modeling language (STS-ml). Our results also show that performing security analysis before safety analysis reveals more safety risks than performing safety analysis first.

The rest of this paper is organized as follows. Section 2 introduces related security and safety co-analysis approaches. Section 3 explains the background of this study. Section 4 presents our study design, study results, and discussions. Section 5 concludes.

2. Related work

2.1 *Security and safety co-analysis approaches*

Safety–security interactions can be classified into four categories (Piètre-Cambacédès, 2010).

- *Conditional dependency: Satisfaction of safety requirements conditions security or vice-versa.*
- *Mutual reinforcement: Satisfaction of safety requirements or safety measures contributes to security, or vice-versa, thereby enabling resource optimization and cost reduction.*
- *Antagonism: When considered jointly, safety and security requirements or measures lead to conflicting situations.*
- *Independency: No interaction.*

A few studies have surveyed safety-security co-analysis methods, e.g. (Chockalingam, 2016) and (Kriaa et al., 2015). Some of the surveyed methods, such as STPA and STPA-Sec (Young and Leveson, 2013), originates from the safety domain and focus on safety analysis first and then security analysis. Some other methods, such as SysML-Sec (Apvrille, 2014), originates from the security domain and performs safety analysis after the security threats are identified.

2.2 STPA and STPA-Sec

The main steps of STPA plus STPA-Sec are:

- Identifying what essential services and functions must be protected or what represents an unacceptable loss.
- Identifying system hazards and constraints.
- Drawing the system control structure, physical hardware, and network structure, and identifying Unsafe Control Actions (UCAs).
- Determining the potential causes of the UCAs. The potential causes could be security vulnerability and threats. To facilitate the security analysis, some guide words like tampered feedback, injection of manipulated control algorithm, and intentional congestion of feedback path, are added (Schmittner et al., 2016). Compared to other security analysis methods, STPA-Sec does not focus on countermeasures that should be taken. STPA-Sec focuses mainly on identifying those scenarios that could lead to losses.

3. Study background

We have performed safety and security co-analysis study (Torkildson et al., 2018) on an autonomous boat using STPA and STPA-Sec. The autonomous boat Revolt shown in Figure 1 was made by Stadt Towing Tank (STT), on a mission from DNVGL in 2014. The model is a 1:20 scale model of the concept ship. The model ship has a length of 3 meters and weighs 257kg.

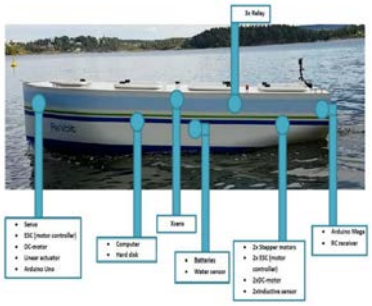

Figure 1. Overview of Revolt and its components

Although Revolt is still under development and is not a fully autonomous boat, we still want to use it as a case since it gives us the opportunity to explore hazard and threats of two main issues i.e., 1) Safety and security of autonomous steering of the ship (i.e., losing control or ship damaged/destroyed) and 2) security of data-communication between onshore and offshore (sensitive data compromised).

When performing STPA plus STPA-Sec analysis, we start with the following unacceptable losses/accidents and safety constraints.

- Collision with vessels, objects, humans/mammals, structures, or grounding
- Fire or explosion
- Foundering (sinking, failing, or plunging)

- Loss of cargo
- Loss of mission objectives
- Loss of information

Then, we read the network structure and the control structure documents of the boat to identify UCAs. We follow the systematic method proposed in (Thomas, 2013) and enumerate full combinations of possible values of process variables and evaluate where control actions can be unsafe if the control action is given, is not given, is given too early or too late, too large or too small value. The Control Actions (CAs) we analyze include:

- CA1: Control the position of the vessel
- CA2: Control the speed of the vessel
- CA3: Control the course of the vessel
- CA4: Control the access to the vessels system

After identifying the UCAs, the last step of the analysis is to identify possible causal factors of the UCAs, including possible security breaches that can lead to the UCAs. In this last step, STPA-Sec analysis is applied by using the guide words proposed in (Schmittner et al., 2016). The security analysis of STPA-Sec focuses on identifying security vulnerabilities that may lead to UCAs. For example, providing CA2 (control the speed of the vessel) too late from shore to the boat when the WIFI connection is jammed.

4. Research design and results

4.1 *Research questions*

The current STPA plus STPA-Sec analysis starts from a safety standpoint. The current STPA-Sec method is performed after STPA and is applied for identifying vulnerabilities that can be the causal factors for safety hazards. Although the current STPA-Sec provides some guide words, based on our lessons learned from the study (Torkildson et al., 2018), we found that some essential security threats can be overlooked by STPA-Sec. We wonder if STPA-Sec can be strengthened by combining with other popular security modeling approaches. So, our first research question (RQ1) is: what is the security threat modeling analysis that can complement STPA-Sec best and easiest? As there are conditional dependency, mutual reinforcement, and antagonism relationship between security and safety, and some incidents, e.g., incidents show in (Guzman, 2015) and (Kamkar, 2013), do show that security of the system is a pre-condition of its safety. We wonder if performing STPA-Sec before STPA may reveal more security threats and UCAs. Therefore, our second research question (RQ2) is: could we start with security analysis, taking a base in the target assets related risks and consequences, and then consider safety afterward?

4.2 *Results of RQ1*

We start by analyzing the possibilities of combining STPA-Sec with existing threat modeling approaches. We have analyzed several popular security threat modeling methods, namely misuse case, data flow diagram, attack tree, BPMN for threats, and Socio-Technical Security modeling language (STS-ml). We first compared the possible advantages and disadvantage of combining those threat modeling approaches with STPA-Sec qualitatively. Then we piloted the combination using Revolt as the case study to see if we can find more security threats than using only STPA-Sec.

4.2.1 Misuse cases

To combine STPA-Sec with misuse case (Sindre and Opdahl, 2005), we need first to identify use cases and then derive misuse cases from the use case diagram. A possible method to identify the use case is to start with existing control actions. The advantage is that converting from control actions to use cases is straightforward. Using misuse cases could help identify vulnerabilities, threats, and malicious actors. However, the disadvantage of the misuse case is that it focuses mostly on high-level threats, which may need to be detailed enough for safety analysis. Thus, combining with the guided words of STPA-Sec, which are more technical, is necessary to identify specific technical threats.

In the Revolt case study, combining a misuse case with the STPA-sec method did help us discover two more possible security-related threats. These threats were related to the data flow and encrypting of the communication part of the system.

4.2.2 Data flow diagram

A data flow diagram is intended to better understand the system ~~via~~ by documenting the data flow between subsystems or different components of the system (Swidersky, 2004). The symbols the diagram uses are intended to show data inputs, outputs, storage points, and the interaction between them. The data flow diagram can help illustrate the attack surface of the system and potentially critical components.

A significant weakness with STPA-sec is that the control loops, which the STPA method focuses on, do not make it natural to cover all the security

features. For example, encryption used for communication may seem to be only relevant to logging and to be not relevant to how the system is controlled. This is what the data flow diagram can strengthen. In addition, we can easily convert the information in the control structure to a data flow diagram. We can just perform one to one mapping of the elements in the control structure of a system, which is the output of the third step of STPA, to corresponding components and data links in the data flow diagram. In the Revolt case study, the control structure of the Revolt is used as a basis for generating the data flow diagram. Figure 2 shows the control structure of Revolt, and Figure 3 shows the data flow diagram derived from the control structure.

The derived data flow diagram of the Revolt helped us identify five more security threats than using STPA-Sec alone. The newly identified security threats are mostly related to the missing encryption between data flows of different components of the control structure.

4.2.3 Attack tree

The attack tree method (Schneier, 1999) produces a tree diagram which illustrated an attack of a system. A typical attack tree will include root (i.e., the goal of the attack), leaves (i.e., various ways in AND or OR relationship to achieve the attack goal). Compared with misuse cases, attack tree analysis can help security analyzers go into very detailed technical aspects of attacks. As STPA-Sec has already guidewords, attack tree method could help analyzer organize the guide words into several layers for more systematic analysis.

In our case of combining the attack tree with STPA-Sec, we found one more threat, which is due to more in-depth analysis of the possible attacks to tamper the WIFI network.

4.2.4 BPMN for threats

The BPMN method is traditionally used for business processes. Using the Business Process Modelling Notation (BPMN) in the context of threats and security analysis has been explored in previous studies, e.g., in the study (Meland and Gjære 2012). The result shows that traditionally, BPMN has been used for regular business processes but could be very suitable for security and threat modeling.

A possible approach to combine BPMN with STPA-Sec is to use BPMN to model the controlled process from the control structure and then find possible threats. In the Revolt case study, the control structure of the Revolt is used as a basis for the BPMN method. The BPMN generated from the control structure is shown in Figure 4.

We analyzed the operation of the embedded computer using BPMN combined with STPA-Sec. The analysis found one new vulnerability, i.e., the possibility to steal information about how the Revolt is maneuvered and what cargo it has. The information can be stolen by installing a keylogger by a malicious operator.

4.2.5 Socio-Technical Security modeling language (STS-ml)

When using the modeling language Socio-Technical Security modeling language (STS-ml) (Trento, 2014), the security analysis could be improved by adding the service-oriented perspective. This is done by adding the information about the services the system provides, in terms of what the goal each actor has and what services exchange information. By doing this, we can relate security requirements to social interactions the system has. We used the basic control structure to create an STS-ml diagram to find the social dependencies through the social interactions the system will be exposed to. An example of STS-ml generated from the control structure is shown in Figure 5.

The STS-ml method shows promising results. However, in the case of the Revolt case study, the STS-ml method did not help us find any new threats related to the social aspect.

For RQ1, we conclude that, among the threat modeling approaches we studied, the data flow diagram seems to be the best to be combined with STPA-Sec, because:

- Generating data flow diagram from the control structure is very straightforward and intuitive.
- Threat modeling analysis based on the data flow diagram complement the biggest weakness of STPA-Sec, i.e., the data flow which is not directly relevant to how the system is controlled could be overlooked in the STPA-Sec analysis. By having a detailed data flow diagram and by analyzing security threats that are related to the data flow, the potential confidentially and integrity issues related to data can be more thoroughly analyzed.
- The other threat modeling approaches can also complement STPA-Sec from different aspects. For example, BPMN can help

identify security threats related to the operation.

4.3 *Results of RQ2*

After we have identified the threat modelling approach to be combined with STPA-Sec, we

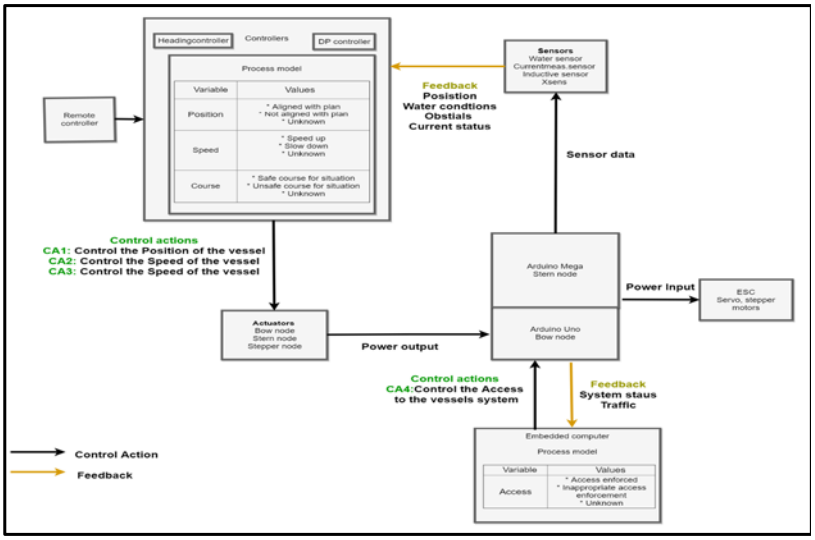

Figure 2. Control structure of the Revolt as a basis for Data Flow Diagram

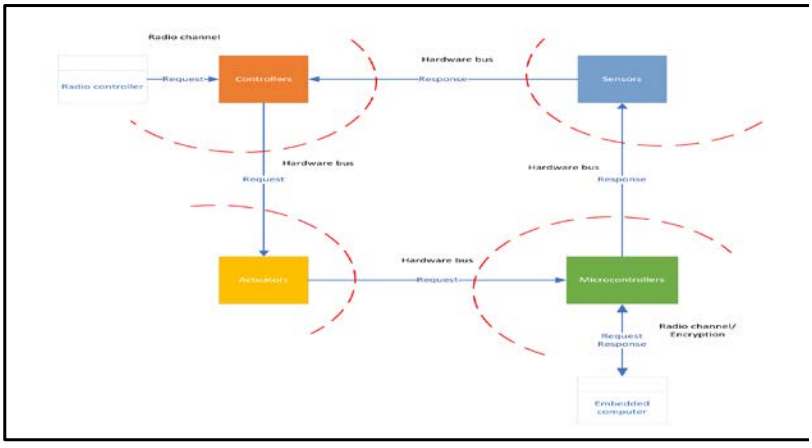

Figure 3. Data Flow Diagram derived from the control structure of Revolt. The control structure is created after safety analysis using STPA

compared the UCAs identified by performing security analysis first versus UCAs we identified in the study by Torkildson et al., (2018). In that study, we applied the traditional way of combining STPA and STPA-Sec, i.e., performing safety analysis first and then security analysis afterward.

first after we have created the control structure. We converted the control structure to a data flow diagram and added some new data flow elements when performing the data flow diagram-based threat modeling. Figure 6 shows the data flow diagram we use for security analysis. It is evident that Figure 6 has more data flow elements than the

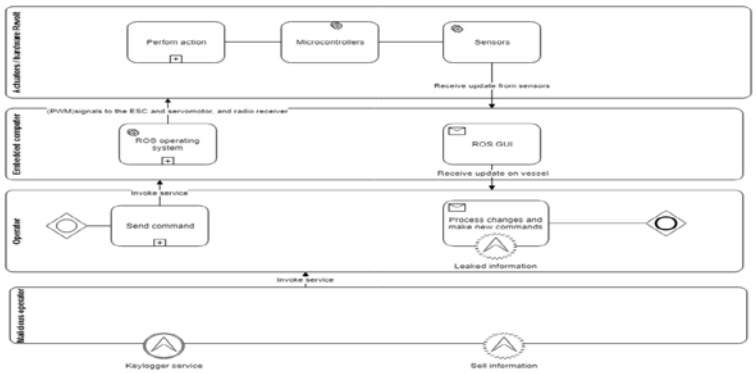

Figure 4. BPMN graph generated from the control structure of Revolt

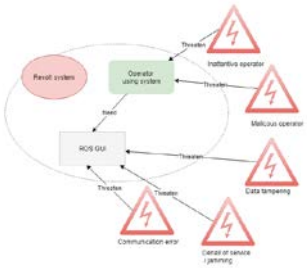

Figure 5. An example of STS-ml generated from control structure of Revolt

As explained in Section 2.2, one step of classical STPA and STPA-Sec analysis is "Drawing the system control structure, physical hardware, and network structure, and identifying Unsafe Control Actions (UCAs)." We perform security analysis

one in Figure 3. The reason for the difference is that when we analyze the security threats based on data flow mindset, we do not limit ourselves to data flow elements that are only directly related to the control of the system. Thus, we identified several data flow elements, such as 4G, which are not directly linked to the control of the system and which could easily be overlooked.

After the security analysis using data flow diagram, we continued the STPA process to identify UCAs. However, the difference is that when we identify UCAs, the security threats identified from the data flow diagram analysis will be considered. After the UCAs are identified, STPA-Sec combined with data flow diagram can be performed again to identify the root causes for the UCAs.

The case study using Revolt show that when performing security analysis first using data flow diagram, we identified more secure communication needs as described in the following. Any compromises of these communications between components of Revolt may lead to UCA.

- Request/receive encrypted messages from the embedded computer to microcontrollers (The microcontrollers are used for handling analog input/output to some of the actuators and sensors)
- Request/receive encrypted messages from the remote controller to controllers
- Request/receive encrypted messages from the remote controller to the embedded computer via GPS/GNSS or WIFI
- Request/receive encrypted messages from sensors, such as video cameras to controllers

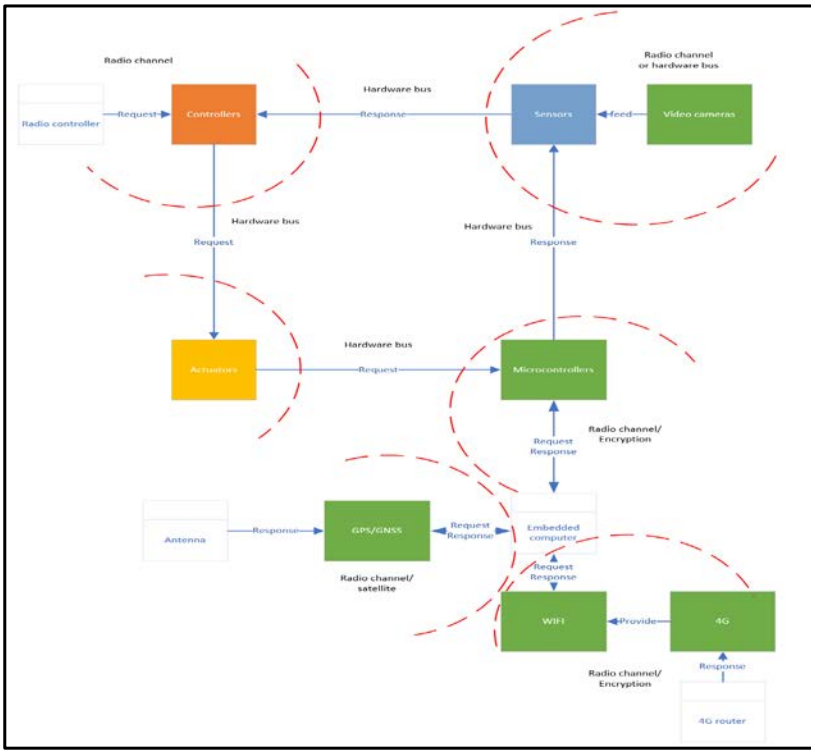

Figure 6. Data flow diagram of Revolt vessel acquired by performing security analysis first

Based on the results of this case study, we would, therefore, recommend performing data flow diagram-based threat modeling before the STPA analysis to identify security analysis first. Then, after the STPA analysis, STPA-Sec can be combined with the data flow diagram again to investigate the possible root cause of UCAs.

5. Conclusions and future work

Many studies have shown that it is necessary to perform security and safety analysis to ensure system safety because security compromise can lead to safety risks. However, many methods start with safety analysis using classical safety analysis methods and then identify possible security threats. The ideas of security analysis of these methods are to figure out whether security compromises are possible root causes of safety risks. If the security compromises are the root causes, the security risks need to be mitigated. In

our previous study, we followed similar ideas and applied the STPA approach to analysis safety risks of an autonomous boat and then applied STPA-Sec to identify root causes of the safety risks coming from potential security breaches.

In this study, we used the same autonomous boat and addressed two research questions, i.e., whether it will be beneficial to also perform security analysis before safety analysis and how to do it in STPA and STPA-Sec context. Our results show clear benefits of performing security analysis before and after safety analysis. In addition, our results show that data flow diagram-based on threat modeling could be a good option to complement STPA-Sec for more thorough security analyses.

Acknowledgment

This work is supported by the SAREPTA (Safety, autonomy, remote control, and operations of industrial transport systems) project, which is financed by the Norwegian Research Council with Grant No. 267860.

References

Apvrille L. and Roudier Y. (2014) "Towards the Model-Driven Engineering of Secure yet Safe Embedded Systems," in Pre-proceedings of the International Workshop on Graphical Models for Security. Available at https://arxiv.org/pdf/1404.1985.pdf

Chockalingam, S., et al. (2016) "Integrated Safety and Security Risk Assessment: A Survey of Key Characteristics and Applications," in Proc. International Conference on Critical Information Infrastructures Security, Springer Springer International Publishing, pp. 50-62.

Guzman, Z. (2015) "Hackers Remotely Kill Jeep's Engine on Highway." Available at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Kamkar, S. (2013) "SkyJack." Available at http://samy.pl/skyjack/.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. & Halgand, Y. (2015) "A Survey of Approaches Combining Safety and Security for Industrial Control Systems," Reliability Engineering & System Safety, 139, 156-178.

Leveson, N. G. (2012) "Engineering a Safer World: Systems Thinking Applied to Safety," MIT Press.

Meland P. H. & Gjære E. A. (2012) "Representing Threats in BPMN 2.0," in Proc. Seventh International Conference on Availability, Reliability, and Security, IEEE Press.

Piètre-Cambacédès, L. (2010) "Des relations entre sûreté et sécurité. (The relationships between safety and security)." Available at https://tel.archives-ouvertes.fr/pastel-00570432/.

Schmittner, C., Ma, Z. & Puschner, P. (2016) "Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis," in Proc. International Conference on Computer Safety, Reliability, and Security, Springer International Publishing, pp. 195-209.

Schneier, B. (1999) "Attack trees," Dr. Dobb's Journal: Software Tools for the Professional Programmer, vol. 24, no. 12, pp. 21-21.

Swidersky S. (2004) "Threat modeling," Microsoft Press.

Sindre, G. & Opdahl, A. L. (2005) "Eliciting Security Requirements ~~W~~with Misuse Cases," Requirements Engineering, 10, 34-44.

Thomas, J.P. (2013) "Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis." (Ph.D. thesis MIT).

Torkildson, E. N., Li, J., Johnsen, S and Glomsrud, J. A. (2018) "Empirical Studies of Methods for Safety and Security Co-analysis of Autonomous Boat," In Proc. of European Safety and Reliability Conference, Taylor & Francis.

Trento, U. O. (2014) "A Social and Organisational Approach to Security Engineering." Available at http://www.sts-tool.eu/.

Young, W. & Leveson, N. (2013) "Systems Thinking for Safety and Security," In Proc. 29th Annual Computer Security Applications Conference, ACM.

Young, W. & Leveson, N. G. (2014) "An Integrated Approach to Safety and Security Based on Systems Theory," Commun. ACM, 57, 31-35.

Formatted: English (United States)