Reconciling Systems-Theoretic and Component-Centric Methods for Safety and Security Co-Analysis

William G. Temple[1], Yue Wu[1], Binbin Chen[1], Zbigniew Kalbarczyk[2]

[1] Advanced Digital Sciences Center, Illinois at Singapore
[2] {william.t, wu.yue, binbin.chen}@adsc.com.sg
[3] University of Illinois at Urbana-Champaign, Illinois, USA
kalbar@crhc.illinois.edu

Abstract. As safety-critical systems increasingly rely on computing, communication, and control, there have been a number of safety and security co-analysis methods put forth to identify, assess, and mitigate risks. However, there is an ideological gap between qualitative system-level methods that focus on control interactions, and more traditional methods based on component failure and/or vulnerability. The growing complexity of cyber-physical and socio-technical systems as well as their interactions with their environments seem to demand a systems-theoretic perspective. Yet, at the same time, more complex threats and failure modes imply a greater need for risk-based analysis to understand and prioritize the large volume of information. In this work we identify promising aspects from two existing safety/security co-analysis methods and outline a vision for reconciling them in a new analysis method.

1 Introduction

As information and communication technology becomes more prevalent in safety-critical systems such as automobiles, trains, and air traffic control, the safety engineering community has confronted the issue of cyber security and its relationship to hazard and risk assessment. While safety and (cyber) security were traditionally considered as separate issues to be evaluated by different subject matter experts, there has been a surge of interest in considering and assessing safety and security in a holistic manner [3, 8, 10]. Such assessments and the risks they identify serve an important role in system design by influencing design decisions and informing the development of assurance cases.

A number of methodologies and techniques have been proposed to integrate safety and security in risk assessment. In some cases, those methods extend familiar safety engineering approaches like failure mode and effect analysis [13] or hazard analysis and risk assessment [9], which evaluate components of a system. Those components are examined to identify hazards, failure modes, and potential vulnerabilities or threats. An alternative approach that has attracted attention in recent years eschews low level hazard and vulnerability assessment and instead focuses on system-level control loops and unsafe control actions [14, 17, 18].

However, while there are a number methods available to analyze the safety and security of a system during the design phase, cyber security threats today are growing ever more complex: they often involve multi-stage attacks, and attackers can exploit physical phenomena in the system and the environment to indirectly cause harm. The classic example of this is the Stuxnet attack, where changes in speed set point on centrifuges caused physical damage to the assets. However the risks posed to systems by cyber-physical interaction are not limited to advanced persistent threats and highly-targeted attacks. In complex systems with hardware and software elements as well as a dynamic physical environment, complex interactions and unintended consequences can lead to hazards. For example, there have been instances of offshore oil rigs temporarily immobilized by malware [4], and a recent metro rail reliability incident in Singapore was due to complex signalling interference between trains triggering fail-safe behavior [16].

Those types of complex interactions are challenging to account for using traditional safety/security analysis methods like fault trees or failure mode and effect analysis. The Systems-Theoretic Process Analysis for Security approach (STPA-Sec) [17], with its emphasis on emergent system behavior and qualitative assessment of unsafe or insecure scenarios may offer one path to addressing these challenges. However, at the same time, more complex threats and failure modes imply a greater need for risk-based analysis to understand and prioritize safety and security issues—a practice eschewed by STPA-Sec. In this work, we seek to bridge the gap between the STPA-Sec approach and those that examine component failure and/or vulnerability in a risk-based manner to address the challenges faced by complex, cyber-physical systems.

2 Review of Safety and Security Co-Analysis Methods

A number of methods have been proposed to improve the completeness of system risk assessment by covering the interactions between both unintentional/non-malicious failures, and intentional/malicious threats. Recent survey and systemization of knowledge papers [3, 8, 10] serve as an excellent starting point to understand the state of the art. In Table 1 we borrow a conceptual framework from recent work [3] to classify approaches as either *extending* an existing method from safety or security analysis (e.g., Fault Tree Analysis, Failure Mode and Effect Analysis), *combining* existing methods (often a safety analysis method and a security analysis method), or proposing an *alternative* method which differs substantially from existing approaches. We add a second dimension inspired by [7], which differentiates whether a method is *component-based* or *systems-based*.

The first group of methods, Security Aware Hazard Analysis and Risk Assessment (SAHARA) [9] and Failure Mode, Vulnerabilities and Effect Analysis (FMVEA) [13] extend existing safety analysis techniques from ISO 26262 [2] and IEC 60812 [1], respectively, by incorporating threat information based on the STRIDE [15] model. The second group, the Failure-Attack-CountTermeasure (FACT) Graph [12], and Extended Fault Tree (EFT) [6] are based on a combination of fault tree and attack tree methods. Combined Harm Assessment of

	Extend	**Combine**	**Alternative**
Component-based	SAHARA[9], FMVEA [13]	FACT Graph[12], EFT[6]	
Systems-based		CHASSIS[11]	STPA-Sec[17], STPA-SafeSec[7]

Table 1: Classification of related work in safety and security co-analysis

Safety and Security for Information Systems (CHASSIS) [11], which involves the combination of use/misuse cases and sequence diagrams, is classified as a systems-based approach because it places more emphasis on interactions between entities (which may include human actors) as opposed to the hardware/software structure of the system. Finally, System-theoretic Process Analysis for Security (STPA-Sec) [17] and the related STPA-SafeSec [7] approaches emphasize a top-down assessment of a system's functional control structure to identify unsafe/insecure control actions.

From Table 1, we see a clear divide between component-based methods that build on classical safety or security analysis techniques and the systems-based approaches which represent a departure from existing standards and traditional thinking. As discussed in the next section, we believe both philosophies have the ability to complement one another to better cope with emerging challenges.

3 Complexity and Unintended Consequences

Safety critical systems today operate in complex environments, with complex failure modes caused by subsystem interdependency and, in many cases, insecure communication and software-based systems. It can be challenging to thoroughly identify threats and hazards during the system design process and even meticulously engineered systems face unanticipated issues during operation. Below we use two recent real-world incidents from the maritime and rail transportation industries to motivate the need for new techniques to analyze safety and security.

Incident 1: Malware disables Offshore Oil Platform In a 2015 speech, an Admiral from the US Coastguard discussed an incident where a mobile offshore drilling platform had its dynamic positioning thrusters disabled by malware [4]. Dynamic positioning thrusters keep a floating drilling platform stationary on the well site by compensating for ocean currents. In this incident, crew members were plugging personal devices such as phones and laptops into the onboard computer system—the same computer system used to control the thrusters. Malware from personal devices entered the system and was able to propagate. Although this was not a targeted attack, unintended interaction facilitated by inadequate cyber security policy and protection caused an unsafe situation where the rig drifted off the well site.

Incident 2: Signalling interference from a nearby train In late 2016, the automated Circle Line train system in Singapore was afflicted with mysterious service disruptions. Trains traveling in multiple sections of the line and directions

would lose the signalling network connection seemingly at random and activate the emergency brake. This persisted for weeks, leading to delays, thousands of inconvenienced passengers, and a serious public relations crisis for the operator. After a detailed investigation involving multiple government agencies and organizations, it was determined that a single train with malfunctioning signalling hardware was emitting a incorrect signals that interfered with nearby trains' connectivity [5, 16].

Both of the above incidents raise questions about the relationship between safety, reliability, and cyber security as well as the manner in which risks to such complex systems are identified and managed. It should be noted that neither incident led to loss of life or serious injury; however system performance and reliability are critical security-related properties that are influenced by and, need to be assessed in conjunction with, system safety and fail-safe behavior.

Several safety/security co-analysis methods introduced in the previous section are intended to address how security threats impact safety. For example, SAHARA [9] and FMVEA [13] incorporate security/threat information into existing safety assessment frameworks. This is desirable from an industry adoption point of view, however are there important system-level threats and consequences that can be overlooked? This may be particularly true for human factors such as the oil rig's crew illegally downloading music, etc. on their personal devices (the reported source of the oil rig malware). Similarly, fault-tree based approaches [12, 6], which are combinatorial, may be unable to adequately cope with complex interactions and interdependencies in a system of systems (e.g., the circle line metro, with multiple driverless trains, trackside power and communication infrastructure, etc.).

Conceptually, the STPA-Sec [17] approach which focuses on the functionality provided by a system, and its functional control structure, rather than on threats and attacker properties, appears well-suited to such systems. However the output of STPA-Sec analysis is qualitative in nature: a list of control actions in the system that may be unsafe or insecure, and how those control actions may lead to unacceptable losses in one or more causal scenarios. This high-level perspective has led to criticism. The authors of [14] point out that STPA-Sec may be more amenable to the early design stages of the system lifecycle since it does not fully align with current safety/security standards—a view shared by [8].

4 Toward a Hybrid Method

We believe there is an opportunity to integrate different aspects of systems-theoretic and component-centric analysis methods. Conceptually, STPA-Sec offers advantages in the identification of complex interactions in the system and environment that may create hazards. However, identifying a large number of interactions and potential sources of loss also lends itself to risk-based analysis: stakeholders need a way to manage that complexity and identify which cyber attacks and/or failures are worth taking seriously. This is where STPA-Sec has limitations. We see potential for a method like FMVEA to play a complementary

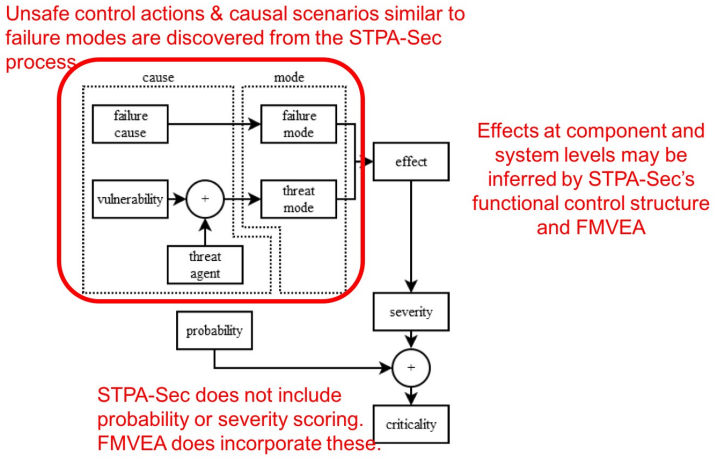

Fig. 1: Annotated FMVEA cause-effect chain highlighting areas where STPA-Sec can be incorporated.

role in supporting the assessment of risk in a structured, semi-quantitative (i.e., numeric rating) manner that considers factors such as severity and likelihood.

We envision a new safety/security co-analysis method that begins with a systems analysis similar to STPA-Sec, which identifies the functional control structure of a system, including the relationships between human actors, the system, and the environment. This may include extensions or modifications to the original STPA-Sec to enhance its coverage of security topics, e.g., [14]. The resulting graphical model of the functional control structure will help stakeholders identify potential risks to reliability, safety, and security.

However, to prioritize and manage the resulting unsafe control actions a more detailed assessment is required. We intend to make use of the process in FMVEA, since it is based on established practices (IEC 60812). Figure 1 shows the information flow in the FMVEA cause-effect chain (see [13]) with annotation to illustrate how information from an SPTA-Sec assessment may be incorporated. Our future work will focus on refining the process for integration, including extensions of the two approaches where appropriate.

5 Conclusion

In this paper, we examine differences between systems-theoretic and component-centric safety/security co-analysis methods. Inspired by two real-world incidents we outline the vision for a hybrid method that combines elements of STPA-sec and FMVEA: two popular approaches from the systems and component side respectively.

Acknowledgments

This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate. It was also supported in part by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A*STAR).

References

1. IEC 60812: Analysis techniques for system reliability procedure for failure mode and effects analysis (FMEA).
2. ISO 26262: Road vehicles - functional safety.
3. S. Chockalingam, D. Hadziosmanovic, W. Pieters, A. Teixeira, and P. van Gelder. Integrated safety and security risk assessment methods: A survey of key characteristics and applications. In *CRITIS*, 2016.
4. CSIS. Coast guard commandant addresses cybersecurity vulnerabilities on offshore oil rigs. https://goo.gl/yJN4xi, 2015.
5. data.gov.sg Blog. How the circle line rogue train was caught with data. goo.gl/qEgy4b, 2016.
6. I. N. Fovino, M. Masera, and A. De Cian. Integrating cyber attacks within fault trees. *Reliability Engineering & System Safety*, 94(9):1394–1402, 2009.
7. I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, 2016.
8. S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, 139:156 – 178, 2015.
9. G. Macher, A. Höller, H. Sporer, E. Armengaud, and C. Kreiner. A combined safety-hazards and security-threat analysis method for automotive systems. In *SAFECOMP*, 2015.
10. L. Piètre-Cambacédès and M. Bouissou. Cross-fertilization between safety and security engineering. *Reliability Engineering & System Safety*, 110:110–126, 2013.
11. C. Raspotnig, P. Karpati, and V. Katta. A combined process for elicitation and analysis of safety and security requirements. In *Lect Notes Bus Inf*. Springer, 2012.
12. G. Sabaliauskaite and A. P. Mathur. Aligning cyber-physical system safety and security. In *Complex Systems Design & Management Asia*. Springer, 2015.
13. C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security application of failure mode and effect analysis (FMEA). In *SAFECOMP*, 2014.
14. C. Schmittner, Z. Ma, and P. Puschner. Limitation and improvement of STPA-Sec for safety and security co-analysis. In *SAFECOMP*, 2016.
15. A. Shostack, S. Lambert, T. Ostwald, and S. Hernan. Uncover security design flaws using the STRIDE approach. MSDN Magazine, 2006.
16. The Straits Times. Train's faulty signals behind circle line woes. https://goo.gl/KbxWpf, 2016.
17. W. Young and N. Leveson. Systems thinking for safety and security. In *ACSAC*, 2013.
18. W. Young and N. Leveson. An integrated approach to safety and security based on systems theory. *Commun. ACM*, 57(2):31–35, Feb. 2014.