Towards Attack Models in Autonomous Systems of Systems

Amer Šurković*, Džana Hanić*, Elena Lisova*, Aida Čaušević*, David Wenslandt† and Carl Falk†
*School of Innovation, Design and Engineering
Mälardalen University, Västerås, Sweden
Email: {asc17003, dhc17002}@student.mdh.se and {elena.lisova, aida.causevic}@mdh.se
†Knightec AB, Sweden
Email: {david.wenslandt, carl.falk}@knightec.se

***Abstract*—In context of safety-critical Systems of Systems (SoS) that are built as a collection of several systems capable of fulfilling their own function as well as the the overall SoS function, increase production efficiency and decrease human effort in such systems, one has to be able to guarantee critical properties such as safety and security. It is not sufficient to analyze and guarantee these critical properties isolated one from another, but one has to be able to provide joint analysis and guarantees on safety and security. This paper is our initial effort towards building a common safety and security assurance approach for complex SoS, where we start from identification and analysis of attack models and connecting them to the already identified functional safety requirements. In this way we will be able to assess system assets and vulnerabilities, and identify ways how an attacker could exploit them. We aim to connect attack modeling process to safety process by aligning mitigation strategies with safety requirements.**

***Index Terms*—safety, security, attack models, systems of systems**

I. Introduction

We are witnessing fast technological and industrial advances within area of autonomous systems of systems (SoS). Systems like SoS are built as a collection of several systems that share their resources and capabilities in order to achieve new functionalities, provide better performance or higher level of efficiency, when compared to traditional systems. It is expected that fully autonomous and cooperating systems increase the production efficiency, and decrease (if not completely replace) the human effort in harmful environments. We can find examples of SoS in different domains such as health, nuclear power plants, automotive, aerospace, construction equipment, etc. In many cases, these systems are also safety-critical, meaning that a failure in such systems could lead to fatal and unacceptable consequences as loss of life, or damage to the equipment or environment [1]. Given that SoS come with higher level of complexity, providing an analysis of its properties and guaranteeing that systems are sufficiently safe and secure is one of the major challenges, since their behavior might evolve due to the dynamic nature of such systems.

Given the fact that SoS include interaction via modern communication infrastructures (i.e., cloud and fog infrastructure), to enable guarantees of critical properties, (e.g., safety and security) it is not sufficient anymore to do their analysis independently, but one has to be able to address safety and security in a joint effort, already at the design time. Safety and security engineering have for a long time been regarded as two separate disciplines, which has resulted in separate cultures, regulations, standards and practices. Already in the 1990s researchers noticed commonalities between safety and security [2], [3], as well as the need to reason about them jointly. Given the facts gathered in the literature, we can state that safety and security are increasingly understood and accepted, but that the state-of-the-practice has not yet reached the same maturity. There is still a significant gap between safety and security practices in the industry, due to separate standards, assessment and assurance processes, and authorities.

The development of safety-critical systems requires engineers to follow strict rules and rigorous processes of safety assurance in order to be allowed to introduce the systems on the market. Such development has to be adapted to changes in systems, and at the same time cater for security-relevant aspects, since a security breach could provoke hazards, be it already identified ones, or completely new hazards. Therefore, a safety demonstration is incomplete and unconvincing unless it considers security. Still, many safety standards do not acknowledge this, potentially resulting in systems certified for safety that are still unsafe due to security vulnerabilities that may jeopardize safety.

This paper is the initial effort towards building a common safety and security assurance approach for complex SoS in which we recognize the need of identifying existing attack models and connecting them to already identified set of safety requirements. In our future work we plan to apply proposed model on an example of autonomous construction site. The aim of this work is to provide an argument that a system is sufficiently safe given that there exists a set of security threats potentially realized through the identified attack models. In this work we choose to analyze system security from an attacker's point of view, and identify how potential vulnerabilities can be exploited.

The paper is organized as follows. In Section II we present the necessary background information with respect to safety and security, as well as attack models. Next, in Section III the proposed approach is described. In Section IV we present related work and position our approach in respect to it. Finally,

we conclude the paper with Section V.

II. Background and Motivation

This section briefly presents security and safety concepts used in this paper, including the notion of attack models.

Security is defined as a system property that allows it "to perform its mission or critical functions despite risks posed by threat" [4]. A threat in its turn can be defined as "the potential source of an adverse event" [4]. A vulnerability is a flow in the system that allows an adversary to realize a threat targeting one of the system assets. A concrete threat realization is an attack. Therefore, once a high-level threat has been identified based on an adversary model, knowledge of the adversary goal and existing vulnerabilities in the system, the threat can be decomposed into possible attacks realizing it.

Safety can be defined as "freedom from unacceptable risk of physical injury or of damage to the health of people" [5]. A system cannot be absolutely safe, but it can be acceptably safe. To define risks, top-level events leading to an accident, i.e., hazards, should be identified. To demonstrate that risks are addressed and minimized to an acceptable level, a safety assurance case is required. A hazards identification procedure and a risk analysis is a part of the case.

Attack models provide a way to analyze system security by deploying a model that considers an adversary point of view, where for each identified system assets one can analyze system vulnerabilities and ways to exploit them, given a certain reward for the adversary.

III. Security Aware Safety Process

In this section we propose to enrich safety process with security considerations by incorporating attack modeling into the safety process. We describe the approach and a rationale behind it.

As it is presented in Fig. 1, given system definition safety process according to ISO 26262 [6] consists from the following steps: (*i*) hazard identification and risk assessment; (*ii*) formulation of safety goals based on hazards of interest; (*iii*) Functional Safety Requirements (FSRs) elicitation aiming to prevent, mitigate or remove hazards; (*iv*) elicitation of Technical Safety Requirements (TSRs) mapped to FSRs. These steps are within the design phase of system development, while software and hardware implementations and further phases are not considered in this paper. Each step of the safety process results in some outcome, e.g., set of hazards or requirements, which we call *artifacts*. The collection of artifacts is continuously updated during the safety process.

To introduce security considerations and particularly investigate how attacks can jeopardize system safety, we introduce attack modeling process incorporated into safety process and propose to use attack modeling process' outcome as an input to the FSRs elicitation step. In this way elicited requirements will include information regarding mitigation techniques for security attacks potentially jeopardizing system safety. The attack modeling process consists of the following steps: (*i*) system assets identification, and the whole process is iterated until all identified assets are considered; (*ii*) next, system needs to be analyzed for its vulnerabilities that could lead to the asset being compromised; (*iii*) then, given a formulated adversary model the reward for breaking an asset is quantified, i.e., risk assessment is performed; (*iv*) finally ways to exploit the vulnerability, i.e., potential threats and realizing them attacks are investigated. The overall outcome of the process is the set of threats and attacks based on which mitigation strategies are developed. Note, as system safety is the overall goal, the input for attack modeling process is not only system definition, but also artifacts derived from safety process. For example, a requirement imposing a monitor as a safety mechanism, can add vulnerabilities to the system and thus needs to be considered during attack modeling process. Hence, once we want to incorporate security considerations while eliciting FSRs, we need to engage the attack modeling process and fed by collected at that moment artifacts to get an input to requirements. However, during the rest of system development process requirements are further refined, thus engaging of attack modeling process can be performed on demand each time we need input on how safety goals of the system can be jeopardized by attacks.

IV. Related Work

In this section we briefly overview related work with respect to common safety and security considerations. We have noticed a significant amount of new approaches proposed, mostly driven by needs in the automotive domain. In majority of cases these approaches are built on already existing approaches, such as HARA [6] coming from the automotive domain and STRIDE [7] focusing on threat modeling to review system design in a methodical way typically used in the security domain, resulting in a Security-Aware Hazard and Risk Analysis (SAHARA) [8]; Failure Modes, Vulnerabilities and Effect Analysis (FMVEA) [9] is a method based on an approach from the safety domain (FMEA), described in IEC 60812 [10] enriched with threats identification; or a method called STPA - Sec [11], which is based on the already existing top-down safety hazard analysis method System-Theoretic Process Analysis (STPA). In most cases these approaches provide parallel reasoning about safety and security, without any feedback between these properties during system lifecycle. Some of the approaches like [12] have a possibility to reuse previously acquired results and redo the analysis in case a new threat or vulnerability is identified. However, this is done not in a continuous manner, and the applicability to more complex and dynamic systems is questionable. SAHARA provides results as quantified security impact on the safety-critical system development. STPA-Sec allows focusing on vulnerable states in order to avoid threats to exploit them and eventual losses. The approach enables parallel consideration of both safety and security properties, as well as single property analysis, however it is not aligned with any standard.

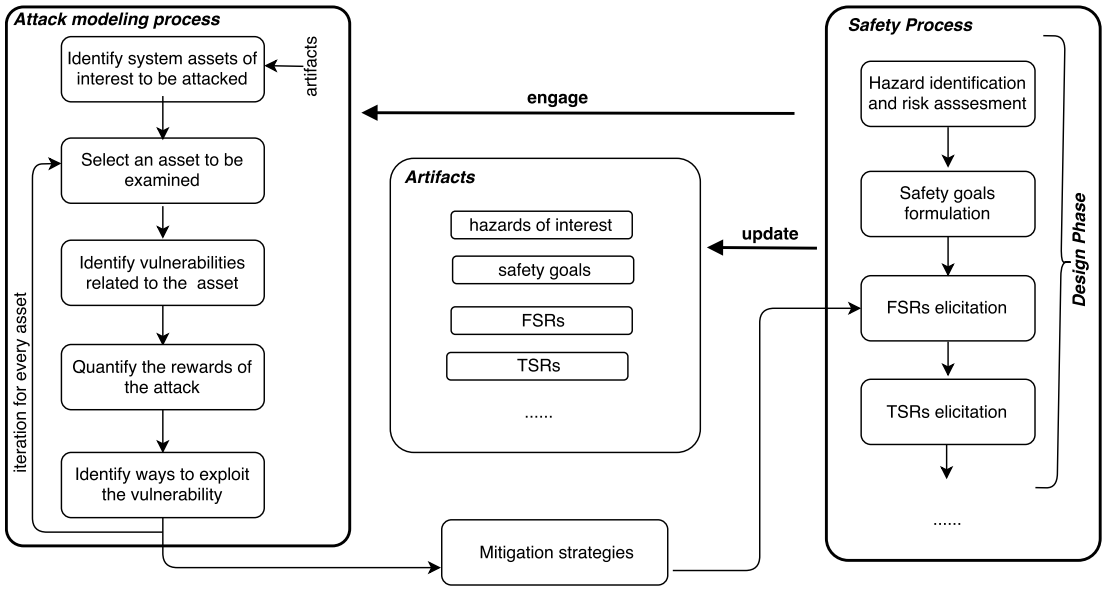

Fig. 1. An approach to incorporate attack modeling process into safety process

Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) is a high level approach that combines safety and security methods in order to provide a joint safety and security assessments approach, usually suitable for early phases of system development [13]. The approach is based on modeling misuse cases and misuse sequence diagrams within a UML behavior diagram. The outcome of the analysis is security and safety requirements specification. Also, by providing a trade-off analysis they check whether there exist mutually dependent or independent features. As it depends on expert knowledge, reusability in repeated analysis is not straight forward [12].

Approaches revised above start from a threat point of view and investigate how threats could be realized by connecting them to potential vulnerabilities and associated attacks. The outcome allows them to implement mitigation techniques. On the other hand in this paper, we are addressing security work from a perspective of an attacker, i.e., based on a system and its assets of interest (to be protected) we consider ways to exploit system vulnerabilities. Furthermore, given safety functional requirements we consider a possible impact from vulnerability exploitation on system safety.

V. Conclusions

This paper is our initial step towards developing a joint safety and security assurance approach. We outline an approach in which we adapt consideration of an adversary point of view through attack models, analyzed for a set of system assets. Our aim is to engage attack modeling process in safety process by providing an iterative feedback between them that will result in accurate updates of system artifacts. In the next step we aim to refine the approach and apply it on an example of an autonomous construction site.

Acknowledgment

This work is supported by the SAFSEC-CPS (Securing the safety of autonomous cyber-physical systems) project funded by The Knowledge Foundation and the SeCRA (Security Case Run-time Adaptation) project funded by Sweden's Innovation Agency Vinnova.

References

[1] J. C. Knight, "Safety critical systems: challenges and directions," in *Proceedings of the 24th International Conference on Software Engineering. ICSE 2002*, May 2002, pp. 547–550.
[2] J. Rushby, "Critical system properties: Survey and taxonomy," Computer Science Laboratory, SRI International, Tech. Rep. SRI-CSL-93-1, 1994.
[3] A. Burns, J. McDermid, and J. Dobson, "On the meaning of safety and security," *Comput. J.*, vol. 35, no. 1, April 1992.
[4] R. Kissel, *Glossary of key information security terms*. U.S. Dept. of Commerce, National Institute of Standards and Technology, 2006.
[5] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, 2011.
[6] International Organization for Standardization, "Iso 26262 road vehicles functional safety part 110," 2011.
[7] Microsoft Corporation, "The stride threat model," 2005.
[8] G. Macher, A. Höller, H. Sporer, E. Armengaud, and C. Kreiner, *A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems*. Springer International Publishing, pp. 237–250.
[9] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, *Security Application of Failure Mode and Effect Analysis (FMEA)*. Springer International Publishing, 2014, pp. 310–325.
[10] International Electrotechnical Commission, "Iec 60812: Analysis techniques for system reliability - procedure for failure mode and effects analysis (fmea)," 2006.
[11] W. Young and N. Leveson, "Systems thinking for safety and security," in *Proceedings of the 29th Annual Computer Security Applications Conference*, ser. ACSAC '13. NY, USA: ACM, 2013, pp. 1–8.
[12] C. Schmittner, Z. Ma, E. Schoitsch, and T. Gruber, "A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security: CPSS 2015*. NY, USA: ACM, 2015.
[13] C. Raspotnig, P. Karpati, and V. Katta, *A Combined Process for Elicitation and Analysis of Safety and Security Requirements*. Springer Berlin Heidelberg, pp. 347–361.