Integrated Safety and Security by Design in the IT/OT Convergence of Industrial Cyber-Physical Systems

1st Amirali Amiri, 2nd Gernot Steindl, 3rd Siegfried Hollerer
Institute of Computer Engineering
TU Wien
Vienna, Austria
firstname.lastname@tuwien.ac.at

***Abstract*—The convergence of Information Technology (IT) and Operational Technology (OT) in Industry 4.0 presents new challenges, necessitating innovative approaches to guarantee the safe and secure execution of production processes. Consequently, the safety and security of production systems have emerged as crucial elements, given that security incidents can result in severe consequences such as production failure, equipment damage, or human injury. Previously, in a stakeholder analysis, we investigated how Austrian industrial automation stakeholders manage safety and security risks. The study, which included vendors, integrators, and asset owners, focused on secure and safe infrastructures, system architectures, and risk management. Our findings revealed limited industry awareness and usage of the Reference Architecture Model Industrie (RAMI) 4.0, emphasizing the need for an economically viable, holistic approach to integrated security and safety by design. Moreover, we introduced a comprehensive ontology for safety, security, and operation requirements in the IT/OT convergence. Building on top of these works, we introduce a model-based engineering approach to implement integrated safety and security while designing industrial Cyber-Physical Systems (CPS). We model these systems precisely using System Modeling Language (SysML) 2.0 specification and verify the requirements.**

***Index Terms*—IT/OT Convergence, Reference Architecture Model Industrie 4.0, Integrated Safety and Security by Design**

I. Introduction

Ensuring security in production systems is vital for safety, reliability, and availability [2]. However, the convergence of IT and OT has created new vulnerabilities, exposing production systems to cyber-attacks [1]. Attacked IT infrastructure may lead to safety issues, system failures, and equipment damage. For instance, exploiting IT vulnerabilities can target a safety instrumented system, resulting in its failure to respond when necessary, or executing safety functions at the wrong time. This can lead to injuries, damage to the production facility, or intentional triggering of safety functions, causing operational stoppages and economic losses [9].

Moreover, measurements to increase safety can lead to security vulnerabilities [12]. For example, to mitigate the possibility of collisions in a cooperative robots application, external devices such as safety sensors equipped with light barriers can be incorporated into the system [4]. However, these sensors necessitate additional network communication, thereby increasing the system's susceptibility to potential security attacks. These examples highlight the necessity for a comprehensive approach to safety and security.

Monitoring the state of production systems and detecting unexpected attacks pose a growing challenge. The complexity arises from the diverse resources, components and the isolated design of safety and security in production systems [2]. Additionally, different perspectives of engineering experts widen the gap in safety and security coverage, complicating the analysis. Although various approaches exist [7], [8], [10], there is a demand for a standardized, flexible framework, and generic tools that seamlessly integrate safety and security in the context of production systems [10].

Previously [5], we examined how stakeholders in Austrian industrial automation firms handle security and safety risks to prevent unfavorable outcomes. The analysis covered product or component vendors, integrators, and asset owners of industrial systems, focusing on safe and secure infrastructures, system architectures, and risk management. Moreover, we identified inter-dependencies between safety and security requirements. The study unfolded in two phases: Initially, an online survey was administered where stakeholders provided simultaneous responses. Subsequently, individual stakeholder workshops were conducted to gather more detailed insights into each stakeholder's OT system and components concerning security and safety considerations, building upon the survey results.

Our findings indicated that the industry was not well-acquainted with and did not widely use the reference architecture RAMI 4.0 [3]. Additionally, the industrial stakeholders under examination expressed a consensus that achieving an economically feasible, comprehensive approach to safety and security by design was an important objective.

In [6], we introduced a comprehensive ontology for safety, security and operation requirements in IT/OT convergence. We identified eight domains to achieve a holistic view on safety and security, i.e., OT domain-specific model, operations and quality, hazard identification, threat identification, safety functions and requirements, security controls and requirements, risk evaluation and prioritization, and risk treatment. In this paper, we build on top of these works and introduce a

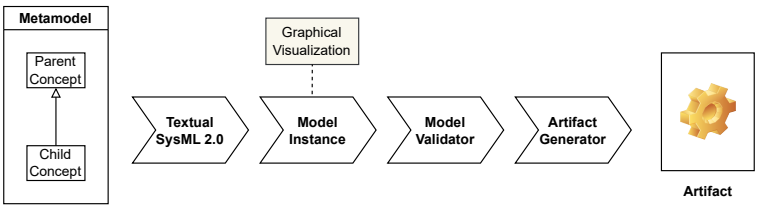

Fig. 1. Model-Based Engineering Approach

Model-Based Engineering (MBE) approach [11] to facilitate the generation of artifacts regarding the integrated safety and security of industrial CPS.

We introduce a metamodel that describes industrial systems with integrated safety and security as a design-time requirement. Our proposed approach adheres to the following steps. Firstly, based on our metamodel, we create model instances using the SysML 2.0 specification[1] to precisely model industrial systems. Secondly, we verify requirements and validate our model instances. Finally, we generate artifacts based on the validated instances.

II. Approach Overview

Model-Based Engineering. Figure 1 shows our MBE approach. We define our *metamodel* (in a combination with our ontological concepts) to describe the industrial systems that must adhere to safety and security guidelines, e.g., IEC 62443[2], which is a series of standards concerning the cybersecurity of industrial automation and control systems. We map this metamodel to the textual representation of the SysML 2.0 specification[1] to create a *Model Instance* [11]. These instances are passed through *Model Validator* that checks the defined safety and security requirements. The validated model instances are then passed to an *Artifact Generator* to generate artifacts, e.g., code, automatic test cases, or recommendation, which are traced back to the requirements.

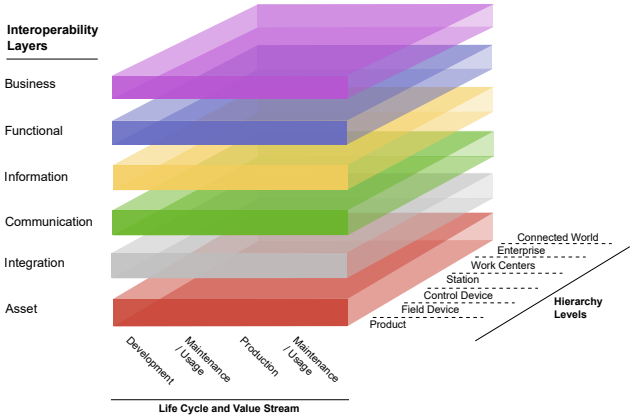

Fig. 2. Reference Architecture Model Industrie 4.0

Reference Architecture Model Industrie 4.0. Figure 2 shows the RAMI 4.0 three-dimensional model [3]. These dimensions are *Life Cycle and Value Stream*, *Hierarchy Levels*, and *Interoperability Layers*. Regarding the *Life Cycle and Value Stream*, our MBE method is used in the *Development Cycle* to generate artifacts implementing the integrated safety and security ontological concepts at the design-time of industrial CPS. These artifacts are used in the *Production Cycle* to ensure safety and security guidelines (e.g., IEC 62443[2]). Regarding the *Hierarchy Levels*, our approach offers benefits at the *Control Device Hierarchy* where safety and security is implemented. Finally, regarding the *Interoperability Layers*, we focus on the *Integration Layer*, where the transition from the real world to the digital world is considered, and the *Communication Layer*, where the communication between different components are mapped. However, we consider all layers in our approach, whenever applicable.

[1]https://www.omg.org/spec/SysML/2.0/Beta1

[2]https://www.iec.ch/blog/understanding-iec-62443

References

[1] M. M. Alani and M. Alloghani. *Security Challenges in the Industry 4.0 Era*. Springer International Publishing, Cham, 2019.

[2] B. C. Ervural and B. Ervural. *Overview of Cyber Security in the Industry 4.0 Era*. Springer International Publishing, Cham, 2018.

[3] R. Heidel. *Industrie 4.0: The reference architecture model RAMI 4.0 and the Industrie 4.0 component*. Beuth Verlag GmbH, 2019.

[4] S. Hollerer, C. Fischer, B. Brenner, M. Papa, S. Schlund, W. Kastner, J. Fabini, and T. Zseby. Cobot attack: a security assessment exemplified by a specific collaborative robot. *Procedia Manufacturing*, 54:191–196, 2021. 10th CIRP Sponsored Conference on Digital Enterprise Technologies (DET 2020) – Digital Technologies as Enablers of Industrial Competitiveness and Sustainability.

[5] S. Hollerer, W. Kastner, and T. Sauter. Safety and security: A field of tension in industrial practice. In *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*, pages 1–7, 2023.

[6] S. Hollerer, W. Kastner, and T. Sauter. Towards a comprehensive ontology considering safety, security, and operation requirements in ot. In *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–4, 2023.

[7] S. Kropatschek, S. Hollerer, D. Hoffman, D. Winkler, A. Lüder, T. Sauter, W. Kastner, and S. Biffl. Combining models for safety and security concerns in automating digital production. In *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*, pages 1–8, 2023.

[8] K. Kurniawan, A. Ekelhart, E. Kiesling, G. Quirchmayr, and A. M. Tjoa. Krystal: Knowledge graph-based framework for tactical attack discovery in audit data. *Computers & Security*, 121:102828, 2022.

[9] J.-w. Myung and S. Hong. Ics malware triton attack and countermeasures. *Int. J. Emerg. Multidiscip. Res*, 3:13–17, 2019.

[10] S. Pirbhulal, V. Gkioulos, and S. Katsikas. Towards integration of security and safety measures for critical infrastructures based on bayesian networks and graph theory: A systematic literature review. *Signals*, 2(4):771–802, 2021.

[11] T. Stahl, M. Voelter, and K. Czarnecki. *Model-Driven Software Development: Technology, Engineering, Management*. John Wiley & Sons, Inc., Hoboken, NJ, USA, 2006.

[12] M. Wolf and D. Serpanos. Safety and security in cyber-physical systems and internet-of-things systems. *Proceedings of the IEEE*, 106(1):9–20, 2018.