Introducing a multi-layered model-based design approach towards safety-security co-engineering

Megha Quamara, Gabriel Pedroza, Brahim Hamid

Introducing a Multi-layered Model-based Design Approach towards Safety-Security Co-engineering

Megha Quamara*, Gabriel Pedroza*, Brahim Hamid†
*Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France
†IRIT - University of Toulouse, 118 Route de Narbonne, 31062 Toulouse Cedex 9, France
Email: {megha.quamara, gabriel.pedroza}@cea.fr, brahim.hamid@irit.fr

***Abstract*—The integration of safety and security concerns in critical domains is of utmost importance, and should be conducted in early design phases of System Engineering (SE) process. However, within a Model-Based System Engineering (MBSE) realm, this goal is hindered by the complex requirement enrichment process across system models/views that often lacks guidance for non-savvy engineers to facilitate integration and verification of stringent safety and security exigencies. In this regard, we present a multi-layered design approach that leverages existing techniques like Model-Driven Engineering (MDE) and formal methods, to facilitate integrated verification of safety and security properties that can be further specialized across different representations (i.e. mission, functional, and component) of a System Under Design (SUD). Our research is in progress and further results are expected to be presented soon.**

***Index Terms*—safety, security, co-engineering, design, model-driven engineering, formal methods**

I. Introduction

The paradigm shift from traditional Industrial Control Systems (ICSs) to software-based systems with intertwined physical elements (e.g., Cyber-Physical Systems (CPSs)) has substantially raised the degree of inter-connectivity, design complexity, and stringency of requirements. Deployment of such systems in critical applications entails integration of safety and security concerns in light of their importance with regards to business, economical, and safety criteria [1]. In such cases, an effective identification and treatment of safety and security risks is crucial, which according to the "correct-by-design" principle, should be conducted at early design stages of the System Engineering (SE) process [2].

Within a Model-Based System Engineering (MBSE) realm, the development process is complex [3] and often lacks guidance for consistent semantic transfer from high-level teleological representation to the detailed technical architecture of the System Under Design (SUD) integrating both safety and security requirements (*issue* **P1**). Moreover, conducting design-level safety-security properties'[1] verification to increase confidence in the system [4], can be error-prone, mainly due to ambiguous properties' specifications or biases introduced by non-savvy engineer's interpretation (*issue* **P2**). Notwithstanding the need for incorporation, existing SE approaches exhibit independent safety and security analyses in many cases [5], [6]. As evident in several safety-critical domains (e.g., automotive), an entanglement exists between safety constraints (e.g., messages' latency) and security exigencies (e.g., encryption mechanisms' overhead), and their mutual assurance needs to be verified [7], specially for critical applications (*issue* **P3**). Nevertheless, a joint analysis towards harmonizing safety-security properties' specifications is technically challenging in practice due to complexity in terms of model size, frameworks/languages involved, proofs' intricacy, etc. A lack of automated tool support for integrated validation and verification of properties is thus observed (*issue* **P4**).

To tackle the above-discussed problematics P1-P4, we have worked on the development of a multi-layered design approach for safety and security co-engineering that shall allow incorporating high-level safety and security requirements into a multi-layer design model, interpreting it into a formalism, and finally, conducting properties' verification in a delegated tool. The key aspects of the approach are detailed in the following section.

II. Proposed Approach

Fig. 1 depicts the overall approach. Globally, it facilitates: (1) specification of a system under design with varying granularity level, and (2) incorporation of safety and security properties via separation of modeling purposes and languages (as opposed to incorporation into a flat single model/view). Accordingly, the system-related aspects can be rendered at following three layers (P1): **Layer 1**, *Mission architecture*, concentrates on the formulation of high-level strategic concerns, called missions, of a complex engineered system, thereby offering a teleological view to capture its overall purpose, **Layer 2**, *Functional architecture*, represents a classical functional decomposition of the system, reflecting the design objectives correlated with its functionality, and **Layer 3**, *Component architecture*, focuses on the low-level detailed technical specification of the target system wherein it is decomposed into a set of components, representing self-contained computational/communication elements or physical entities.

The idea behind the aforementioned layered representation is driven by the aim to provide design choices and cover critical system-related aspects allowing safety-security properties' analysis. Herein, the allied conceptual models are the cornerstone that (1) encompasses fundamental notions, their attributes, and potential relationships for stating the structural and behavioral aspects of the SUD, and (2) endows models

[1]Fundamental well-defined notions that are the building blocks upon which high-level requirements can be decomposed and characterized.

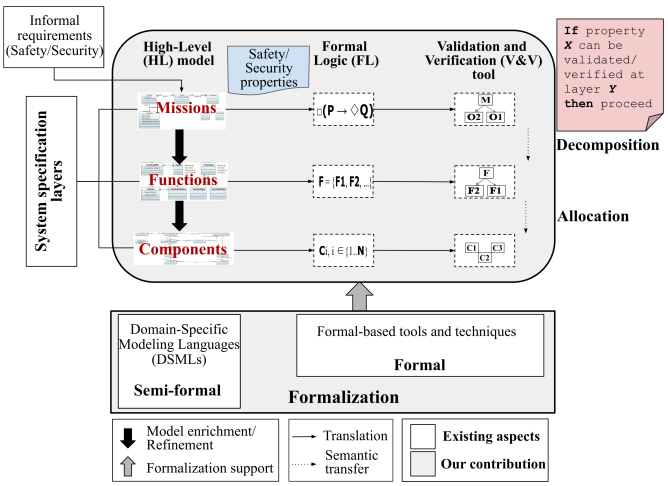

Fig. 1. Overall multi-layered model approach.

with a semantics to allow verification of properties. Yet standalone defined, layers' semantics should still be consistent and thus amenable for both top-down or bottom-up design strategies, whereby models' formalization shall allow progressive detailing of the SUD (i.e., WHAT-HOW-WHICH) and in particular malfunctioning propagation, attack progression, etc.

Integrated Design Approach for Safety and Security. With the layered conceptual models as its foundation, the approach aims at encompassing the "safety- and security-by-design" principle, disambiguation in properties' specification, and early detection of conflicts between properties in the SE process (P3). This is accomplished via (1) *modeling* of detailed system aspects and safety-security properties, (2) *formalization* of both system aspects and properties, (3) *integration* of formalized model elements, and (4) *verification* of properties via transformation into a delegated formal tool. Once formalized, the properties' specifications (instantiated at the three model layers) remain generic enough to be accommodated as reusable libraries, as depicted in Fig. 2. The approach has been already instantiated for mission-centric and component architecture layers, and a proof-of-concept was developed based upon a Connected Driving Vehicles (CDVs) case study [8].

Languages and Techniques for Modeling and Formalization. The multi-layered specification language for the proposed approach supports system design at two levels: (1) semi-formal - relying upon technology-agnostic, generic, and standardized constructs to create Domain-Specific Modeling Languages (DSMLs) for system's graphical representation, and (2) formal - based upon formal syntaxes, semantics, and rules for sound specification, reasoning, and verification of properties (P2). A tool-chain support architecture based upon Model-Driven Engineering (MDE) techniques (namely Eclipse Papyrus) and formal-based tools (namely Rodin and Alloy analyzer) is developed and its main features include SUD-properties modeling, verification of design conformity with respect to the properties, and inconsistencies' detection (P4).

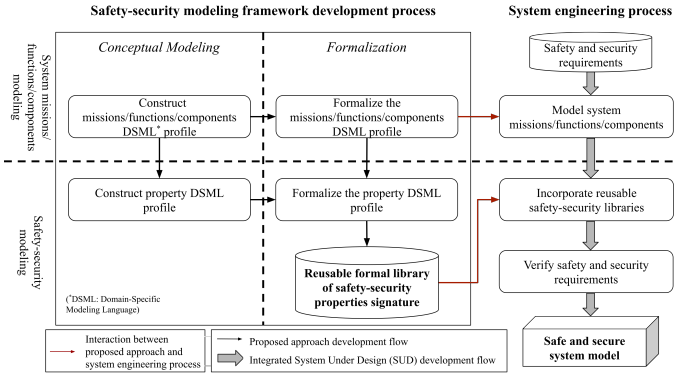

Fig. 2. Methodology for the creation of integrated design and analysis framework pertaining to safety and security.

III. Conclusion and Work Perspectives

This paper introduced a multi-layered model-based design approach for integrated specification and analysis of safety and security properties. An instantiation of the approach for mission-centric and detailed component architecture layers demonstrates its feasibility and leverages reusability of safety-security properties' signatures across different design projects. Preliminary results are expected to be published soon. Being the framework generic and technology-agnostic, it shall facilitate model transformation towards other formal-based tools, thus alleviating the complexity of manually integrating formal analysis of safety and security aspects during the design phase.

As a work-in-progress, the foreseen actions for approach consolidation include (1) the instantiation of the *Functional* layer of system specification, and (2) the improvement of vertical integration between the layered DSMLs. In this last regard, the intertwined semantics of the layered DSMLs imposes challenges, for preserving properties' consistency across layers, necessary to ensure soundness of top-down and bottom-up design strategies' application.

References

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*. IEEE, 2008, pp. 363–369.

[2] M. Wolf and D. Serpanos, "Safety and security in cyber-physical systems and internet-of-things systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 9–20, 2017.

[3] J. A. Estefan *et al.*, "Survey of model-based systems engineering (MBSE) methodologies," *Incose MBSE Focus Group*, vol. 25, no. 8, pp. 1–12, 2007.

[4] S. Zafar and R. G. Dromey, "Integrating safety and security requirements into design of an embedded system," in *12th Asia-Pacific Software Engineering Conference (APSEC'05)*. IEEE, 2005, pp. 8–pp.

[5] M. A. De Miguel, J. F. Briones, J. P. Silva, and A. Alonso, "Integration of safety analysis in model-driven software development," *IET software*, vol. 2, no. 3, pp. 260–280, 2008.

[6] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous vehicle: Security by design," *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[7] G. Pedroza, "Towards Safety and Security Co-engineering: Challenging Aspects for a Consistent Intertwining," in *Security and Safety Interplay of Intelligent Software Systems*. Springer, 2018, pp. 3–16.

[8] D. Firesmith, "Engineering safety-and security-related requirements for software-intensive systems," Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, Tech. Rep., 2007.