Multi-View Design for Cyber-Physical Systems

Hui Zhao, Ludovic Apvrille, Frédéric Mallet

Multi-View Design for Cyber-Physical Systems

Hui Zhao [1] Ludovic Apvrille [2] Frédéric Mallet [1]
[1] Université Côte d'Azur, I3S, INRIA
[2] Telecom ParisTech, CNRS/LTCI Sophia Antipolis, France

March 2017

Abstract

Cyber-Physical Systems are complex systems made of various and heterogeneous subsystems; they have different aspects and each aspect has its own requirements and properties to be satisfied. Model-Driven Engineering (MDE) is a promising approach used to design and analyze complex systems on different levels and diverse views. CPS designers take many factors into account due to the complexity and diversity of current CPS systems. The designers have their own individual experience and specific viewpoint; they may use different models and languages to describe various domains, different models and languages lead to a complex coherency management. Therefore, how to promote the coherency of a whole system and ensure all subsystems can work together is an important concrete issue.

To resolve this issue, we introduce a unified modeling methodology which can coordinate different models and languages with a multi-view approach. Indeed, we expect multi-view approaches to help handling system coherency. Hence, we focus on providing a high-level modeling methodology with multi-view that (i) Coordinates different languages of models and diverse tools. (ii) Ensures engineering-wide collaboration by sharing the same reference architecture. (iii) Handles the complexity of systems and architectures, using unified viewpoints to model the whole systems with top-down refinement. (iv) Supports different formal methods to verify critical elements. (v) Backtraces verification results to models.

keywords CPS, MDE, Heterogeneous Modeling, Multi-View Design

1 Introduction

Cyber-Physical Systems (CPS) are highly complex and widely distributed systems. CPS are made of heterogeneous subsystems that include cyber computational parts and physical processes. The cyber part is made of discrete elements and the physical part is mostly continuous. In an entire and complex system, those two aspects are combined. In other words, cyber-physical systems include the intersection of the physical and computational parts, and their interactions

[10]. Also, physical components are very different from computational systems in several ways. Therefore, in contrast to model a computational system, cyber-physical systems combine engineering models and methods from mechanical, electrical, aeronautical and industrial engineering with the models and methods of computer science. It is for these qualitative differences that some coherence problems emerge [9] and make it more difficult fo design complex and heterogeneous. Thus, It is a common practice to use a modeling language for each sub-domain: Domain Specific Modeling Languages (DSMLs) have been introduced for that goal. Recently, several contributions [3] [4] have proposed new ways approaches to deal with several specific domain languages together. However, a systematic design must coordinate the different languages to understand the emerging system behavior, and there are still gaps of syntax and behavioral semantic.

To overcome this difficulty, we explore a coordination approach that allows coordinating different models which are described by DSML, thereby, providing a possibility to analyze and unify the design of complex systems effectively. Moreover, our approach is able to consider a lot of different properties and views of a system from a global viewpoint. Larsen *et al.* [15] have shown a first step in that direction, we follow this same path while focusing more on different views and aspects, such as safety and security views.

This paper is organized as follows. In section 2 we present the motivations for our research work. Then, section 3 illustrates our methodology of multi-view design using a railway signaling system as a case study and gives preliminary meta-models. In Section 4, we explore some significant views and discuss further work. In this paper, we tried to concise and clear point out the direction of our researches and proposed the method of implementation way, therefore, we do not attempt to give a complete and concrete example, but rather subpart of our case study that are relevant for the scope of this paper.

2 Motivation and Objective

The goal of our research is to build a bridge between system models and inner models at different abstraction levels of the system (as shown in Fig.1), i.e., a set of components whose interaction semantics is usually informal, and the heterogeneous (more concrete) components that are expected to satisfy some of the system's properties. By leveraging some of the properties obtained on the component level, we hope to offer mechanisms useful for the integration stage: verify that components satisfy with system requirements, allow substitution of components and exploration of alternative costs with regards to both their functional and non-functional properties. Meanwhile, we intend to conduct execution, verification and validation activities at system level.

Our research on system modeling view was inspired by existing Model-Based System Engineering (MBSE) methodology and approaches (SysML/MARTE and Arcadia/Capella). Existing MDE frameworks, e.g. Eclipse Modeling Tool [1],

[1] Eclipse modeling tool web page: http://www.eclipse.org

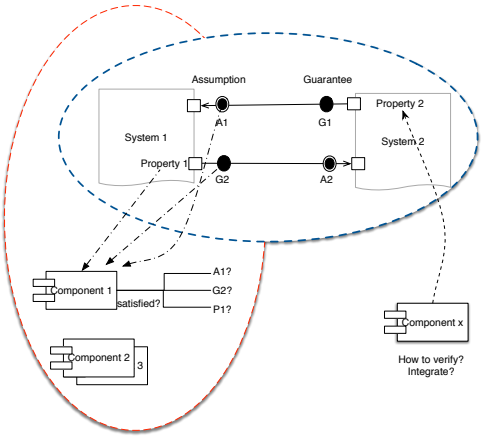

Figure 1: Horizontal and Vertical system view

integrate various analysis techniques supporting the engineering process within a common environment. The EMF is used to capture meta-models as a high-level abstract model. Moreover, we rely on TTool [1] to model the system and perform security and safety proofs.

- ARCADIA/Capella project [2], ARCADIA and Capella are Model-Based System Engineering (MBSE) [14] methods and tool suites for designing systems from a high level of abstractions, ARCADIA/Capella also adopts a multi-view point description to illustrate different specifications, such as physical part, logical part, and allocation relationships. ARCADIA/Capella has been successfully deployed in a wide variety of industrial contexts.

- UML and its profile for the embedded system called MARTE [1] are applied for modeling on a high-level, and a set of formal methods help system engineers to verify the main and safety-critical components, which are imperative procedures to guarantee the quality of the system.

- TTool is a free and open-source support toolkit supporting several profiles, including SysML-Sec [2]. TTool offers diagrams for capturing system requirements, modeling software/hardware partitioning and performing performance/security/safety proofs support model transformation techniques. For security and safety proofs, TTool relies on *ProVerif* and *UPPAAL*, respectively.

We consider the connections between modeling and meta-modeling aspects (UML/SysML) regarding the combination of Real-Time and Security/Dependability

[1] http://ttool.telecom-paristech.fr/index.html
[2] https://www.polarsys.org/capella/arcadia.html

Figure 2: Arcadia Methodology

points of view. There is certainly a strong feedback from each on the other (if only to mention that they may conflict as security may add latency to computations). Notions of mixed-criticality and the time variations of trust zones according to change of system states are other examples of this. We intend to put here the emphasis on proper and insightful modeling of these aspects, as a preamble to analysis and verification of joint temporal and security/safety conditions. We want to illustrate these issues based on potential use cases of a railway signaling system connecting several subsystems.

3 Methodology and case study

ARCADIA is a MBSE method for the system, handling both hardware and software architectural concepts. It enforces a methodology structured on four successive engineering phases which separate needs (operational need analysis and system need analysis) and solutions (logical and physical architectures), (Fig.2), in accordance with IEEE1220 standard.

According to this method, we give the definition of each phase, and sketch meta-models using the Eclipse Modeling Framework (EFM)[1]. Meanwhile, we apply this method to the railway signaling system and related subsystem in an industrial field.

3.1 Operational Analysis

At the Operational Analysis phase, we should capture the Operational Activities and Operational Entities and the interactions between them. The activities include functional and non-functional properties such as partitioning, safety, security. Finally, it can describe and structure the needs and the goals of the customer. The meta-model of our approach is given in Fig.3.

[1]https://www.eclipse.org/modeling/emf/

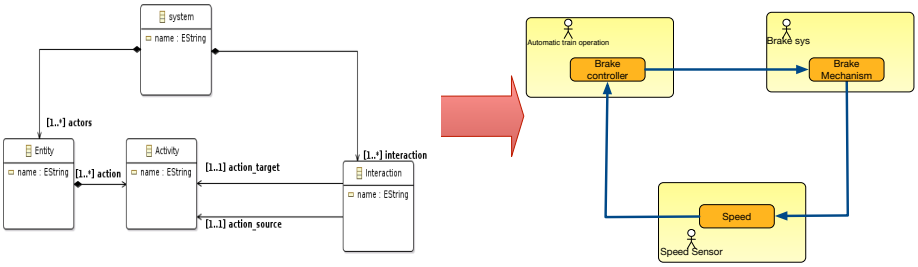

Figure 3: Meta-Model of Operational Analysis

3.2 System Analysis

At the System Analysis phase, we focus on the system level. An architecture is intended to illustrate allocations (Fig.4) of functions onto components so as to comply with systems' needs. Meanwhile, the architecture diagram is also used to check the feasibility of the customer requirements with a multi-view approach (safety, cost, consumption, etc,.).

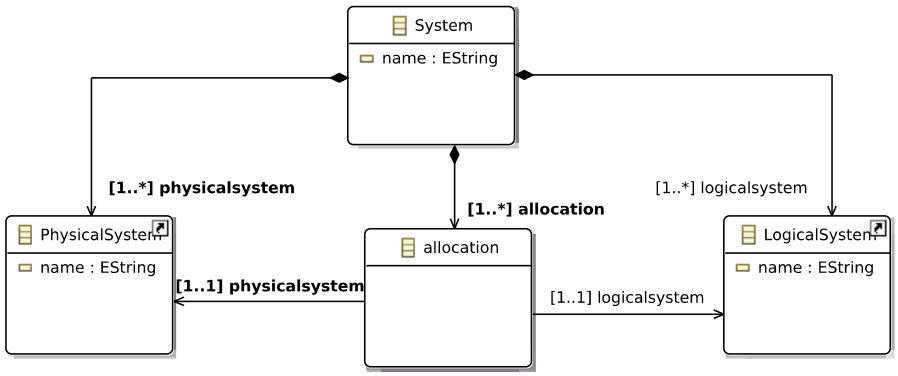

Figure 4: Allocation on system level

3.3 Logical Architecture

This step aims at building a coarse component breakdown of the system which is not challenged in the further development process. All the functional and non-functional constraints (safety, security, performance, cost, non-technical, etc.) are taken into account, starting from previous functional and non-functional analysis refined results (functions, interfaces, data flows, behaviors, etc.), building one or several decompositions of the system into logical components.

3.4 Physical Architecture

The Physical Architecture step is similar to logical architecture design procedure. It consists of the selected physical architecture which includes components to be produced, formalization of all viewpoints and how they are taken into account in the components design. Once the model has been finished, a more classical development stage can start. The same viewpoint-driven approach as for logical architecture design is used.

4 Related work

Multi-view design, as proposed by Gomez *et al.* [6], relies on `MARTE` and `SysML` in order to focus on power view and the relationship between functional, non-functional and structural aspects. we noticed that Persson *et al.* [13] has analyzed the relation of views and taken the characterization from three main perspectives for the relations of viewpoints, semantic (content), relations over time (process), and manipulation of views (operations).

Moreover, Fang *et al.* [11] have given a formal definition of the multi-view model at the meta-model level, and then they proposed a unified graphical environment and toolkit for CPRS modeling. Also, Kienzle *et al.* [8] discussed an aspect-oriented modeling approach called RAM. RAM makes the models more scalable to multi-view modeling by using 3 modeling notations (UML class diagrams, state and sequence diagrams).

5 Future work and Discussion

Most CPS systems are safety-critical systems. Model-Driven Engineering allows analysis of system parts from the simulation of behavior to better predict failure modes.

Our research has been inspired by former work about assessment and evaluation of a system's *Safety integrity level*. During the last years, researchers were wondering how to find an "ideal" MDE approach which is able to support safety analysis (SA) methods [12] automatically according to a set of standards such as EN61508 [7]. Safety-critical systems are expected to demonstrate a high level of dependability, and in particular safety. Therefore, standards [7] concerned with the development of such systems define a specific system life-cycle where system engineering is conducted in parallel with SA. Each phase of SA implies the application of specific methods and activities. Typical SA methods include hazard analysis, Fault Tree (FT) generation and analysis (FTA), Failure Mode and Effects Analysis (FMEA) [5].

Once a view such as the safety analysis view has been completed, it should be integrated into the system architecture view. Furthermore, the modeling environment should offer capabilities for safety analysis that also takes into account the architecture. Finally, we focus on the integration of some of the

views into existing MDE tools (e.g. TTool) and show how system modeling can be coupled with safety analysis capabilities in a seamless environment.

References

[1] UML profile for MARTE: modeling and analysis of real-time embedded systems. pages 1–754, June 2011.

[2] L Apvrille and Y Roudier. SysML-sec: a sysML environment for the design and development of secure embedded systems. *APCOSEC*, 2013.

[3] Muhammad Waqar Aziz and Muhammad Rashid. Domain Specific Modeling Language for Cyber Physical Systems. In *2016 International Conference on Information Systems Engineering (ICISE)*, pages 29–33. IEEE, 2016.

[4] Benoît Combemale, Julien DeAntoni, Benoit Baudry, Robert B France, Jean-Marc Jezequel, and Jeff Gray. Globalizing Modeling Languages. *Computer*, 47(6):68–71, 2014.

[5] IEC 60812 Technical Committee. IEC 60812, Analysis Techniques for System Reliability-Procedure for Failure Mode and Effects Analysis (FMEA), 2006.

[6] C Gomez, J Deantoni, and F Mallet. Multi-view power modeling based on UML, MARTE and SysML. *Software Engineering and ...*, 2012.

[7] International Electrotechnical Commission IEC. Functional safety of electrical/electronic/programmable electronic safety related systems. *IEC 61508*, 2000.

[8] Jörg Kienzle, Wisam Al Abed, and Jacques Klein. *Aspect-oriented multi-view modeling*. ACM, New York, New York, USA, March 2009.

[9] Edward Lee. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. *Sensors*, 15(3):4837–4869, February 2015.

[10] Edward A Lee. Cyber Physical Systems: Design Challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing*, pages 363–369. IEEE, 2008.

[11] Fang Li, Jiafu Wan, Ping Zhang, and Di Li. A multi-view integration modeling approach for cyber-physical robot system. In *2013 International Conference on Machine Learning and Cybernetics (ICMLC)*, pages 387–392. IEEE, 2013.

[12] Faida Mhenni, Nga Nguyen, and Jean-Yves Choley. Automatic fault tree generation from SysML system models. In *2014 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM)*, pages 715–720. IEEE, 2014.

[13] Magnus Persson, Martin Törngren, Ahsan Qamar, Jonas Westman, Matthias Biehl, Stavros Tripakis, Hans Vangheluwe, and Joachim Denil. A characterization of integrated multi-view modeling in the context of embedded and cyber-physical systems. *EMSOFT*, 2013.

[14] Pascal Roques. MBSE with the ARCADIA Method and the Capella Tool. *8th European Congress on Embedded Real ...*, January 2016.

[15] Matias Ezequiel Vara Larsen, Julien DeAntoni, Benoît Combemale, and Frédéric Mallet. A Behavioral Coordination Operator Language (BCOoL). In *2015 ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (MODELS)*, pages 186–195. IEEE, 2015.