An Integrated Approach to Formal Analyze Cyber Physical Systems

Riad Helal [1], Akram Seghiri [1] and Faiza Belala [1]

[1] *LIRE Laboratory, Constantine 2 University, Constantine 25000, Algeria*.

Abstract

Very large-scale systems now and in the future will be built by integrating existing systems from different providers to create 'systems of systems' (SoS). Cyber Physical Systems (CPS) constitute an example of these complex systems, including computation, communication, and control. The complexity of CPS engineering arises when cyber capabilities communicate and coordinate with the physical capabilities (sensors/actuators). Several challenges should be overcome to design these systems, especially those related to their modeling and formal analysis. For this purpose, our doctoral research aims to propose a new approach for specifying CPS structures in a formal way facilitating their behaviors analysis. We opt to use the SysML model in order to bring the CPS designer closer to the theoretical models, based in this case on Maude language, which will serve as a formal basis for the analysis of these systems, in particular their security aspect, which currently constitutes a major challenge in all their application fields.

Keywords

Cyber physical systems, Formal Analysis, HI-Maude, SysML.

1. Context

Cyber-Physical System (CPS) is an emerging concept currently trending in many industries. A cyber-physical system (CPS), as its name suggests, is an integration of computation (software) with physical processes. Its behaviour is also defined by both the cyber and physical parts of the system [01]. CPSs are considered as complex systems including computation, communication, and control (3C) technology (Figure1), where the cyber capabilities communicate and coordinate with the physical capabilities (sensors/actuators), in a similar but more sophisticated way to the Internet of Things (IoT) [2].

Tunisian Algerian Conference on Applied Computing (TACC 2022), December 13 - 14, Constantine, Algeria
EMAIL: riad.helal@univ-constantine2.dz (A. 1); akram.seghiri@univ-constantine2.dz (A. 2); faiza.belala@univ-constantine2.dz (A. 3)
ORCID: 0000-0003-2689-5036 (A. 1); 0000-0002-1760-1932 (A. 2); 0000-0002-4563-4061 (A. 3)

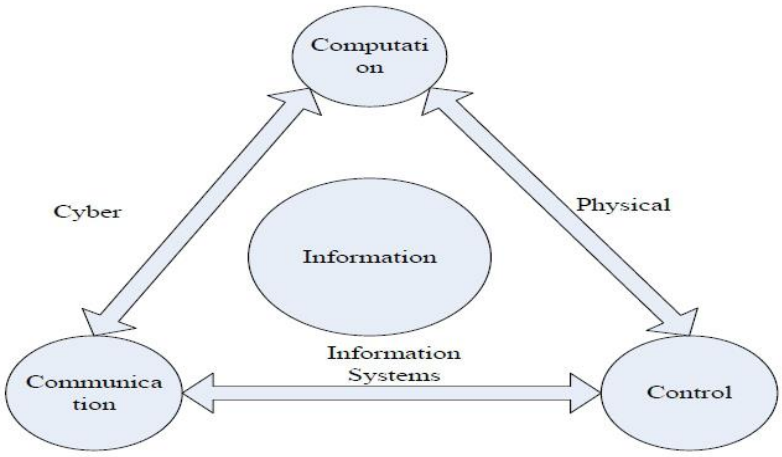

Figure 1: The 3C conception of CPS [3].

These systems have been integrated as a core foundation in many critical infrastructures as well as other domains, in order to improve the day-to-day life quality. Domains may include Military, Industry, Transportation, Healthcare, Agriculture, etc.

CPSs are different from desktop computing, traditional embedded systems, real-time systems, and Wireless Sensor Networks (WSNs) [4]. CPSs are distinguished by several characteristics: diverse nature of their elements, high number of heterogeneous components, high autonomy, decentralization, computational capability, interoperability, connectivity, communication, and networking capability [05]. Designing a CPS poses unique challenges due the requirement to represent their numerous characteristics. Therefore, reliable approaches are needed for the design of these complex systems. For this purpose, we are interested in our doctoral research in proposing an approach to formally specify CPS structures, and to analyze their behaviors.

Our work aims at providing an addition to filling the gap around CPS design challenges (by dealing with both the cyber and physical aspects), by providing a model encoded in Systems Modeling Language (SysML), as a conceptual model to describe CPS constituents. Then, the obtained model is formalized using the Maude language, its HI-Maude extension specifically, serves as a tool to specify, implement and execute this model.

SysML was designed by the International Council on Systems Engineering (INCOSE) and the Object Management Group (OMG), as a profile for UML2.0 [06]. In [07], Hause et al. defined SysML as: ” SysML is a visual modeling language that extends UML 2 in order to support the specification, analysis, design, verification and validation of complex systems that include components for hardware, software, data, personnel, procedures and facilities” [07].

On the other hand, HI-Maude is a recent formal modeling language, and an analysis tool for complex hybrid systems, based on rewriting logic [08].

The rest of the paper is organized as follows: In Section 2, we discuss an overview of the recent work on CPS modeling, we indicate some CPS modeling challenges and limitations that motivated our approach. Research goals are presented in Section 3. In Section 4, we explain our proposed approach. We give our expected contribution in Section 5 before concluding with final remarks in Section 6.

2. Problem Statement

CPSs are systems that include cyber processes and physical processes. Their complex infrastructure and their large number of components, makes their modeling and verification very difficult. It gets more difficult to verify that connections between components are valid as a model becomes more complex [09], another challenge; by incorporating problems like inconsistent time

measurements, network delays, imprecise communication, consistency of views of system state, and distributed consensus, modeling distributed systems increases the difficulty of modeling CPS [09]. With the arising challenges involving CPS, due to the rapid growth in computational technology and hardware industry, proposing designing methodologies that deal with their specification, management, and their analysis is not a trivial matter.

To fill in this gap, there have been several approaches in the literature that have addressed CPS design. In the work conducted by [10], CPS is argued to have the intersection issue of cyber and physical problems, thus the authors offered models that include these both element types. They identified two complementary approaches, the first approach designed to model and design CPS called “cyberize the physical”, referring to wrapping software abstractions around physical sub-systems, and the second is a complementary approach called “physicalize the cyber” which aims at endowing software and networking components with abstractions suitable for physical sub-systems.

In [11], Rajhans et al. proposed an extension to an existing software architecture tool for modeling physical systems of a CPS, through interconnections and interactions between physical and cyber components. They created a new CPS architectural style to support the main design and evaluation of alternative architectures for CPS.

The use of SysML to model CPSs has been discussed in different contributions. For instance, [12] designed and implemented an integrated modeling and co-simulation toolchain, called HybridSim, for the design and simulation of CPS. First, this framework is able to transform and import existing system components from many domains into SysML. Secondly, from SysML designs, HybridSim can generate configuration scripts and Functional Mock-up Units (FMUs). Finally, HybridSim can co-simulate these FMUs in accordance with the Functional Mock-up Interface standard. they used a comprehensive hydronic heating system model for Smart Buildings as a case study to demonstrate the convenience and efficiency of their framwork.
Similarly, authors in [13] proposed a SysML-based modeling methodology, for the systematic construction of testable models of CPSs, and an efficient co-simulation framework called ” SysML-Simulink2”. They validated the suitability of their approach with an industrial case study from the satellite domain.

In the same thought, and to address the emerging need for platform and languages that can accommodate both system and software development processes in CPS, [14] introduced a foundational and executable subset of SysML (fsysML) aimed to ease the development of modern CPS. fSysML defines a textual surface language for a subset of SysML, and integrates this subset with an executable subset of UML.

In [15], Xie an al. presented an integrated SysML modeling and verification approach to cover the specification of nominal behavior of Safety-critical CPS (SC-CPS). Compositional verification is performed to verify the nominal behavior of the SysML model, while FTA (Fault Tree Analysis) is used to do the safety analysis based on the "Safety Profile" of SysML. The Guidance, Navigation, and Control (GNC) system is used as an industrial case study to demonstrate the efficiency of their methodology.

Among the existing works that support security aspects in CPS during the modeling phase, authors of [16] presented an approach based on a model encoded in SysML for security analysis of CPS in the design phase. They proposed a framework that characterizes a distinctive collection of attributes for each given subsystem in a CPS. These attributes build well-formed models that allow the security posture of the system they define to be evaluated. Their proposed framework is based on the evaluation of historical vulnerability data from databases, referred to as evidence, which is then applied to the system model based on those attributes.

Authors in [17] and [18], presented solutions based on formal methods. For instance, the work presented in [17] discussed a method for building models of Petri-nets for cyber-physical attacks, The method is based on the principle that small detailed attack Petri-net models can be created separately

by different security domain experts, instead of building a large single Petri. The main step of the construction method unifies the separated Petri nets using a model description language. A proof-of-concept Python application is used to demonstrate the novel modeling technique for an example assault against smart meters. In [18], a solution is proposed as a multi-cyber framework based on the Markov model to increase the availability of CPS. They proposed a CPS with several cybers in the computing unit to improve the availability and reliability of the system.

However, despite advances in the modeling area and the existing modeling approaches dedicated to specify CPS, there still a lack of powerful formal semantics that support the continued behavioral analysis of CPSs, capturing their evolutionary nature, and having enough expressiveness to describe these complex systems.

3. Research Goals

This doctoral research aims at addressing the designing issues around CPS, by providing a solution to support the characteristics of CPS in terms of their complexity. Our solution gives a formal modeling approach of CPS, tackling their structural (cyber and physical) constituents on one hand, and their evolutionary behaviours on the other.

We propose an approach of specification and integrated analysis, based on several aspects: functional, structural, topological and behavioral.

We will develop a research activity aimed at providing mathematical frameworks, methods and tools to design and formally analyze the CPS. Particularly, we plan, on one hand, to continue the theoretical and fundamental studies in the field of the Maude language through their recent extensions (HI-Maude) in order to provide a powerful formal analysis, and on the other hand, the use of the different diagrams of SysML language (Requirement diagram, Structure Diagrams, Behavior Diagrams) to model CPS.

4. Proposed Approach

We propose an integrated approach to formally specify and analyze CPS. Its definition process is divided into two complementary phases, illustrated in Figure 2, which will answer the kept research questions:

(1) Modeling CPS components using the SysML language and its various attributed diagrams, offering a visual and graphical view of these components and their relations, in a comprehensive way.
(2) The proposed SysML model is then formalized using the Maude language, and its extension HI-Maude specifically, where CPS structures are specified, analyzed, and executed.

The use of SysML is justified by its wide utilization by systems engineers, as it was designed specifically for systems engineering to model large complex systems containing cyber and physical components. SysML's semantics are more prosperous and more flexible, and it offers a robust, simple, and easy framework for systems modeling.

Maude (and its extension HI-Maude) is a language based on rewriting logic; it provides modeling and formal analysis of complex hybrid systems with combined discrete and continuous behavior. With this powerful tool, the user only has to specify the continuous dynamics of single components and single interactions, instead of having to explicitly define the continuous dynamics of the system.

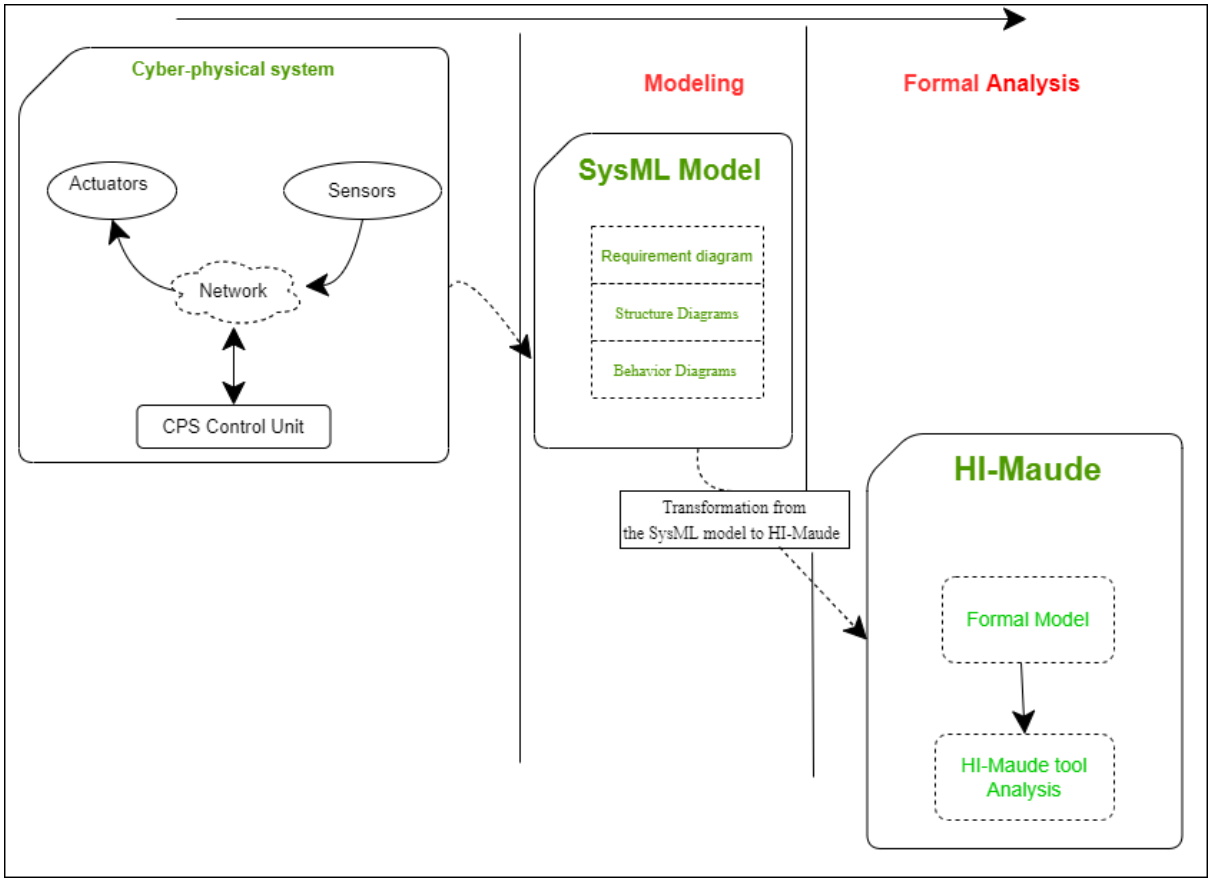

Figure 2: Proposed Approach

5. Expected Contribution

In the context of CPS design, the expected contribution of this doctoral research is to define a new approach that supports the specification and formal analysis of CPS. Our Approach takes the study of the cyber part and the physical part of CPS conjointly. In this context, we will be able to model a CPS with SysML, as a first step, and in the second step transform the SysML model into HI-Maude for a formal analysis. Thus, we obtain two CPS complementary models.

Therefore, it is necessary to identify the requirements and characteristics of our methodology, carry out a comparative study of the existing solutions in the context of the identified requirements, situate our approach as a solution, and finally carry out a case study with a real CPS, making our results more effective and accurate.

6. Conclusion

This paper discussed the design challenges of CPS, manifested by the various characteristics of these systems (complexity, heterogeneity, etc.). The complexity and heterogeneity of CPSs make their design very difficult. We have achieved a literature review, leading to the conclusion that there is lack of appropriate formal approaches and formalisms that model and analyze CPS, on both the structural and behavioural levels. To fill in this gap, we have set a number of goals that need to be achieved in order to tackle this research question.

In an attempt to reach these goals, we gave some approach steps to formally analyze CPS. First, we propose a CPS modeling using SysML language and its different diagrams. Then, we translate the resulting model in Maude language and its extension Hi-Maude, offering a rigorous and formal specification of CPS and their evolving behaviours, which can be executed and analyzed.

Future work may include means and tools to formally verify the coherence of the proposed approach, and its ability to deal with other aspects of CPS such as security.

7. References

[1] E. A. Lee and S. A. Seshia, Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, 2017.

[2] Rad, Ciprian-Radu; Hancu, Olimpiu; Takacs, Ioana-Alexandra; Olteanu, Gheorghe (2015). "Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture". Conference Agriculture for Life, Life for Agriculture. 6: 73–79.

[3] Wan, K. et al. (2011). "Investigation on composition mechanisms for cyber physical systems," International Journal of Design, Analysis and Tools for Circuits and Systems, vol. 2, no. 1, August 2011, pp. 30-40

[4] Wan, J., Yan, H., Suo, H., & Li, F. (2011). Advances in cyber-physical systems research. KSII Transactions on Internet and Information Systems (TIIS), 5(11), 1891-1908.

[5] Napoleone, A., Macchi, M., & Pozzetti, A. (2020). A review on the characteristics of cyber-physical systems for the future smart factories. Journal of manufacturing systems, 54, 305-335.

[6] Xie, Jian, et al. "SysML-based compositional verification and safety analysis for safety-critical cyber-physical systems." *Connection Science* 34.1 (2022): 911-941.

[7] Hause, M. (2006, September). The SysML modelling language. In *Fifteenth European Systems Engineering Conference* (Vol. 9, pp. 1-12).

[8] Fadlisyah, M., Ölveczky, P. C., & Ábrahám, E. (2011, November). Object-oriented formal modeling and analysis of interacting hybrid systems in HI-Maude. In International Conference on Software Engineering and Formal Methods (pp. 415-430). Springer, Berlin, Heidelberg.

[9] Derler, P., Lee, E. A., & Sangiovanni-Vincentelli, A. L. (2011). Addressing modeling challenges in cyber-physical systems. CALIFORNIA UNIV BERKELEY DEPT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE.

[10] Lee, E. A. (2010, June). CPS foundations. In Design automation conference (pp. 737-742). IEEE.

[11] Rajhans, A., Cheng, S. W., Schmerl, B., Garlan, D., Krogh, B. H., Agbi, C., & Bhave, A. (2009). An architectural approach to the design and analysis of cyber-physical systems. Electronic Communications of the EASST, 21.

[12] Wang, B., & Baras, J. S. (2013, October). Hybridsim: A modeling and co-simulation toolchain for cyber-physical systems. In 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications (pp. 33-40). IEEE.

[13] González, C. A., Varmazyar, M., Nejati, S., Briand, L. C., & Isasi, Y. (2018, October). Enabling model testing of cyber-physical systems. In Proceedings of the 21th ACM/IEEE international conference on model driven engineering languages and systems (pp. 176-186).

[14] Badreddin, O., Abdelzad, V., Lethbridge, T., & Elaasar, M. (2016). fSysML: Foundational Executable SysML for Cyber-Physical System Modeling. In GEMOC@ MoDELS (pp. 38-51).

[15] Xie, J., Tan, W., Yang, Z., Li, S., Xing, L., & Huang, Z. (2022). SysML-based compositional verification and safety analysis for safety-critical cyber-physical systems. Connection Science, 34(1), 911-941.

[16] Bakirtzis, G., Carter, B. T., Elks, C. R., & Fleming, C. H. (2018, April). A model-based approach to security analysis for cyber-physical systems. In 2018 Annual IEEE International Systems conference (SysCon) (pp. 1-8). IEEE.

[17] Chen, T. M., Sanchez-Aarnoutse, J. C., & Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid. IEEE Transactions on smart grid, 2(4), 741-749.

[18] Parvin, S., Hussain, F. K., Hussain, O. K., Thein, T., & Park, J. S. (2013). Multi-cyber framework for availability enhancement of cyber physical systems. Computing, 95(10), 927-948.