Addressing Verification and Validation Challenges in Future Cyber-Physical Systems

Nuno Laranjeiro*, Camilo Gomez†, Enrico Schiavone‡, Leonardo Montecchi§,
Manoel J. M. Carvalho¶, Paolo Lollini‖** and Zoltán Micskei††
* CISUC, Department of Informatics Engineering, University of Coimbra, Portugal
†Centro para la Optimizacion y Probabilidad Aplicada (COPA)
Departamento de Ingenieria Industrial, Universidad de los Andes, Bogota, Colombia
‡ResilTech S.R.L, Italy,
§Institute of Computing, University of Campinas, Brazil,
¶Instituto Nacional de Pesquisas Espaciais – Centro Regional Nordeste (INPE-CRN)
‖University of Florence – Firenze, Italy
**Consorzio Interuniversitario Nazionale per l'Informatica (CINI), University of Florence – Firenze, Italy
††Department of Measurement and Information Systems, Budapest University of Technology and Economics, Hungary
*cnl@dei.uc.pt, †gomez.ch@uniandes.edu.co, ‡enrico.schiavone@resiltech.com, §leonardo@ic.unicamp.br
¶manoel.carvalho@inpe.br, ‖**lollini@unifi.it, ††zoltan.micskei@mit.bme.hu

***Abstract*—Cyber-physical systems are characterized by strong interactions between their physical and computation parts. The increasing complexity of such systems, now used in numerous application domains (e.g., aeronautics, healthcare), in conjunction with hard to predict surrounding environments or the use of non-traditional middleware and with the presence of non-deterministic or non-explainable software outputs, tend to make traditional Verification and Validation (V&V) techniques ineffective. This paper presents the H2020 ADVANCE project, which aims precisely at addressing the Verification and Validation challenges that the next-generation of cyber-physical systems bring, by exploring techniques, methods and tools for achieving the technical objective of improving the overall efficiency and effectiveness of the V&V process. From a strategic perspective, the goal of the project is to create an international network of expertise on the topic of V&V of cyber-physical systems.**

***Index Terms*—Cyber-physical Systems, Verification, Validation**

I. Introduction

Cyber-physical systems (CPS) integrate computation and physical parts in a seamless manner. Indeed, they are characterized by a very strong relation between the software part and the physical part (i.e., the environment and conditions that are external to the system, including humans) and are built precisely to support that kind of relation. Such systems are now at the center of people's lives and are being used in a variety of domains, such as aeronautics, energy, healthcare, or transportation [4]. In many cases, cyber-physical systems are supporting complex business or mission-critical operations where a failure may lead to disastrous consequences.

There are several **challenges**, brought by the next-generation of cyber-physical systems and related with the assurance of functional and quality attributes, for which there are no adequate solutions in the state of the art. Indeed, many times the applied solutions are ad-hoc or based in trial and error [6]. The presence of complex relations between both parts of the system, makes it difficult to characterize or estimate the impact of the (also complex) external conditions. In addition, in many cases it is impossible to reproduce a certain environment for testing purposes, which means that there are less opportunities for obtaining assurances regarding a certain quality of the system and calls in for new V&V approaches.

A difficult aspect is related with the growing complexity of current software and especially the use of the components with non-deterministic behavior where traditional verification activities are difficult to apply (e.g., software based on machine learning, with non-explainable outputs). Other classes of systems include self-adaptive systems, which create different obstacles to the verification activities, namely the fact that the system itself changes throughout the time, based on the environment, previous knowledge and current and past states of the system.

The increasing use of new and complex runtime middleware to suport CPSs operations adds complexity between the application and the hardware or the operating system underneath. This applies to virtualization technologies, including plain virtual machines or more light-weight virtualization mechanisms such as containers, for which a number of quality properties must be properly assured (e.g., isolation between containers, security, robustness of the APIs involved). If such technologies are used in a cloud computing context, properties like elasticity must be assured, if the context is edge computing properties like latency, mobility support, or privacy may be difficult to assure, especially if we consider the complex environment interactions involved.

CPSs are often built based on a composition of many other independent autonomous systems. The constituent systems are used as means to achieve a higher goal (which none of the

This work has been supported by the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No 823788.

constituent systems by itself would be able to achieve). Such concept is named Systems-of-Systems, for which the literature has identified numerous challenges, including dynamicity, evolution and emergency properties, which are simply aggravated by the context in which CPSs tend to operate.

Finally, V&V activities fit classic development processes, like waterfall, rather well. However, traditional V&V activities are not a good fit for modern software development processes, where software is developed in an incremental and iterative manner. Thus, one of the challenges is related also with the way CPSs are built and verified, especially with the way the verification activities integrate with the pure development phases.

The abovementioned key challenges are to be tackled by the project ADVANCE [1], funded by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Actions Research and Innovation Staff Exchange (RISE), grant agreement No 823788. Project partners include: Consorzio Interuniversitario Nazionale Per L'Informatica (CINI), Italy with the local node at the University of Florence (CINI-FI); University of Coimbra, Portugal; Budapest University of Technology and Economics (BME), Hungary; Universidad de los Andes (UNIANDES), Colombia; ResilTech s.r.l., Italy; University of Campinas (UNICAMP), Brazil; and National Institute for Space Research (INPE), Brazil.

II. Reference Use Cases

The ADVANCE project activities will focus in two main use cases (UC1 and UC2). **UC1** is the *Brazilian Environmental Data Collection System* (BEDCS), which is maintained by the National Space Research Institute of Brazil (INPE), and it is essentially an environmental data collection system that includes three segments: space, ground, and user [2]. The space segment consists of satellites equipped with hardware and software for collecting data; at the ground level, stations for receiving data and a mission centre for processing and distributing data to end users; and the user segment is composed of about eight hundred platforms geographically distributed across Brazil (in land and at sea) that use sensors to collect environmental data. Data is registered in a database at the mission center, processed, and made available to users via a web interface.

UC2 is the second identified use case and refers to the *validation of safety-critical open-source operating systems for large-scale CPS deployments*. This use case, which is owned by Resiltech, Italy, is set around the OSADL SIL2LinuxMP project [5] whose goal aims at the certification of an embedded GNU Linux real time operating system, according to established standards, namely IEC 61508, which is at the basis of the most relevant safety standards used nowadays.

III. Project Objectives

The **scientific objective** of the ADVANCE project is the definition of new approaches to allow the Verification and Validation of Cyber-Physical Systems (CPS). In order to achieve this goal, the project consortium is researching new techniques, methods, and tools to improve the effectiveness and efficacy of the V&V process. ADVANCE will focus on two main aspects of V&V. The first aspect is related with the definition of techniques to collect evidences of the quality (in *lato sensu*) of a cyber-physical system (this will involve research on system modelling, testing, fault forecast, and structured procedures like failure mode and effect analysis). The second aspect is related with the techniques that allow to manage and analyse data of this type of systems (including data related with the development process used, like requirements management, or traceability).

The ADVANCE project also has the **strategic objective** of creating an international network of expertise and collaboration in the context of V&V of cyber-physical systems. Besides allowing the consortium to reach the project's scientific objectives, the established relations allow training students and professionals in V&V and with respect to the state of the art. Besides the technical challenges described in the first section of this paper, it is important to notice that skilled professionals in V&V, software testing, and Information and Communication Technology (ICT) are currently lacking, at a world level [3]. So, within the project scope, training material is to be produced on the topic or V&V of cyber-physical systems and based on the project outcomes. The fact that the project consortium brings together V&V experts which have different skills and different backgrounds is a strong foundation for creating synergies and for very targeted transfer of knowledge and collaboration.

Expected outcomes include the opportunity for carrying out joint research work, which allows exploring the heterogeneous expertise found across the consortium; the mobility opportunities which are the basis for supporting collaborative research; obtaining new skills on areas like fault injection, systems of systems, model-driven engineering, software and system design, or anomaly detection; the creation of training materials across different domains; and transfer of knowledge to the industry. Overall, ADVANCE aims at improving the European, Brazilian, and Colombian scientific excellence in the area of verification and validation of cyber-physical systems.

References

[1] H2020 ADVANCE: Addressing Verification and Validation Challenges in Future Cyber-Physical Systems. http://advance-rise.eu/, 2019 [Accessed October 1, 2019].

[2] M. A. Chamon. Scientific and Technological Satellites at INPE/BRAZIL. In *57th International Astronautical Congress*. American Institute of Aeronautics and Astronautics, 2012.

[3] European Commission. High-Tech Leadership Skills for Europe – Towards an Agenda for 2020 and beyond. Final Report prepared to the European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, March 2017.

[4] National Science Foundation. Cyber-Physical Systems (CPS). Technical Report NSF 19-553, February 2019.

[5] Open Source Automation Development Lab. OSADL Project: SIL2linuxmp, 2019.

[6] X. Zheng, C. Julien, M. Kim, and S. Khurshid. Perceptions on the State of the Art in Verification and Validation in Cyber-Physical Systems. *IEEE Systems Journal*, 11(4):2614–2627, December 2017.