High Assurance on Cyber-Physical Interactive Systems

Rui Couto[0000−0002−9214−3767] and José C. Campos[0000−0001−9163−580X]

Department of Informatics/University of Minho & HASLab/INESC TEC
Braga, Portugal
{rui.couto, jose.campos}@di.uminho.pt

Abstract. Cyber-Physical Systems, as distributed systems of computational elements interacting with the physical world, are highly complex systems. They can, in many instances, be considered safety critical interactive systems, as errors in interaction can have disastrous consequences (consider the case of autonomous vehicles or integrated clinical environments). High assurance is, then, an underlying requirement, also at their user interface. In this position paper we identify five challenges to be solved both in the short and in the long term, regarding the modelling of (1) distributed and (2) heterogeneous interactive systems, (3) the analysis and relation between the different abstraction layers of Cyber-Physical Systems, (4) the modelling of real time/hybrid systems, and (5) the modelling of the dynamic nature of such systems. Solutions for these challenges are not presented, but possible directions are discussed.

Keywords: Cyber-Physical Systems, Interactive Systems, Formal Methods

1 Modelling and verifying Cyber-Physical Systems

Cyber-Physical Systems (CPS) are networked and/or distributed systems of computational elements interacting with physical processes in feedback loops. CPS are composed of heterogeneous elements, some of which might support interaction with users (*humans*) through different means, from traditional graphical user interfaces to different types of sensors. In these cases, we can consider them to have humans in the loop, as part of the systems themselves. Examples include autonomous driving vehicles and Integrated Clinical Environments (ICE) (see [13] for a state of the art). These are also two examples of systems that require some degree of user interaction to operate.

According to Accord Market, the global market share of CPS has reached the order of million US$ in 2018, and its further expansion is expected [6]. CPS such as Advanced Driver-Assistance Systems (ADAS) or autonomous driving vehicles, which aim not only to improve the driving experience, but also to increase driving and road safety, are being pushed forward by market demands. These demands have raised a set of challenges to be addressed in the short term [11], as these systems are already in usage. Solving these challenges is of major relevance, as the occurrence of errors has serious consequences, such as incidents occurring with autonomous driving vehicles[1].

In [10] a number of challenges related to developing user interfaces for CPS is identified, from the lack of standardized interaction hardware, to appropriate development process and tools. Here, however, we focus specifically on the design analysis aspect. In particular, when the need to assure the safety of the systems is present. Many of these systems can be considered critical (interactive) systems, as they allow the users to perform potentially dangerous actions. Due to their complex nature, their verification is far from a trivial process. Intuitively, it is possible to understand that adding multiple communicating devices will further increase the complexity of the analysis process, when compared with traditional systems.

Model-based approaches allow developers to create models describing the systems to be analyzed, in which (semi-)automated analysis approaches can be applied, such as model checking or theorem proving (i.e. formal verification methods). CPS, being complex systems, require appropriate modelling and verification techniques, in order to reduce the possibility of error. Formal model-based verification approaches for CPS have been discussed, both in terms of challenges and of concrete proposals for analysis. General challenges are discussed in [14], while [12] discusses challenges expected in modelling autonomous driving vehicles. Concrete proposals include model-based analysis, but also co-simulation and testing [4], as well as proposals for anomaly detection [5]. These works focus mainly in the modelling of the behavior and intercommunication aspects, but lack consideration of the human-computer interaction angle. This paper highlights the challenges related with model-based approaches applied to the user interaction aspects of these systems.

In the case of interactive systems, model-based approaches have also been developed to verify interaction properties. An example is the IVY workbench [1], which provides a language to specify interactive systems, a compiler to support the verification of the language with the NuSMV model checker [2] and visualizations to present the analysis result, as well as simulation features. The PVSIO-web tool [8] presents a different approach, both in the formal analysis process, which resorts to the PVS theorem prover [9], and in the support for model inspection, providing tools that support building prototypes from the models. The CIRCUS tool suite [3] supports the modeling of interactive systems, with an emphasis in task modelling and analysis. An effort was made to provide tools which support the modelling process, at different abstraction levels. In general, current approaches focus mainly in the validation of single user-system interactions. However, interaction in CPS is not provided by a single interface, but rather by different computational elements.

[1] `https://www.tesla.com/blog/what-we-know-about-last-weeks-accident`, last visited July 15, 2019.

2 Modelling and verification challenges

An initial exploration has been done in [7], regarding the interactive components of CPS in the context of ICE systems, which already provides some understanding of the expected challenges. While the authors explored the adoption of existing techniques to handle CPS, the challenge itself is bigger than just applying existing approaches, multiplied by the number of communicating devices, plus a communication challenge. Thus, regarding the application of model-based approaches to the interactive components of CPS, five main challenges are expected to be faced:

Distributed interactive systems — The nature of CPS implies the existence of distributed (interactive) systems, and consequently distributed interfaces of systems cooperating between themselves. This results in the challenge of modelling those systems and interfaces, but more interestingly, in modelling their properties. We need to understand what is specific about them and how it can be specified, and which properties can be specified and/or verified. Such requires investigating appropriate languages and tools.

Heterogeneous interactive systems — CPS are composed of several devices, which can interact with users through distinct approaches, such as graphical user interfaces, physical elements (e.g. buttons), or motion sensors. The heterogeneity of the resulting user interfaces can, ultimately, lead to the need to create different modelling approaches, in order to support, for instance, analysis and prototyping. Further research is required in the CPS context.

Different abstraction levels — CPS can be specified at different specification levels, as, for instance, the device layer, the communication layer, and the network layer. As user interfaces are built on top of these layers, their analysis can ultimately be affected by the capability of analyzing each of the layers. While this increases the complexity of modelling these systems, it increases the complexity of their analysis as well. Considering the challenges imposed by CPS, existing tools and approaches should be analyzed in this context, in order to understand their suitability to address each of these layers.

Modelling real time/hybrid systems — Due to the critically of these kinds of systems, the application of real time verification techniques is expected. Such can easily become an issue, since current verification techniques present scalability issues. Furthermore, the computational components are typically discrete in nature, while the physical process are continuous. As a result, how best to model and analyze the real time and hybrid dimensions of user interfaces for CPS, and their relevant properties, needs to be investigated.

Dynamic systems — CPS are prone to changes in the network, with the inclusion/removal of nodes. An example is Vehicle-to-Vehicle (V2V) communication, where vehicles constantly enter and exit the range of other vehicles. Thus, the existence of a specific vehicle in the system is not guaranteed. The same is true for an ICE system, where devices can be added/remove as well. Thus, the dynamic aspect of the network should be taken in consideration. This is expected to impact the behavior of the interactive systems, and consequently, how they are modelled.

3 Conclusion

Model-based approaches have been successfully used to improve the reliability of software systems, as well as of interactive systems. The dissemination of CPS has raised new concerns, currently not addressed by existing solutions. This position paper described five challenges that are expected to be found while developing new approaches for modeling and dealing with user interfaces for CPS. Facing them, ultimately requires researchers to combine the previous acquired knowledge in model-based approaches and CPS, in order to develop new approaches.

Acknowledgments

This work was financed by National Funds through the Portuguese funding agency, FCT - Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) within project: UID/EEA/50014/2019.

References

1. Campos, J.C., Harrison, M.D.: Interaction engineering using the IVY tool. In: Proceedings of the 1st ACM SIGCHI symposium on Engineering interactive computing systems. pp. 35–44. ACM (2009)
2. Cimatti, A., Clarke, E., Giunchiglia, E., Giunchiglia, F., Pistore, M., Roveri, M., Sebastiani, R., Tacchella, A.: NuSMV Version 2: An OpenSource Tool for Symbolic Model Checking. In: Proc. International Conference on Computer-Aided Verification (CAV 2002). LNCS, vol. 2404. Springer, Copenhagen, Denmark (July 2002)
3. Fayollas, C., Martinie, C., Palanque, P., Deleris, Y., Fabre, J.C., Navarre, D.: An approach for assessing the impact of dependability on usability: application to interactive cockpits. In: 2014 Tenth European Dependable Computing Conference. pp. 198–209. IEEE (2014)
4. Fitzgerald, J., Gamble, C., Larsen, P.G., Pierce, K., Woodcock, J.: Cyber-Physical Systems Design: Formal Foundations, Methods and Integrated Tool Chains. In: 2015 IEEE/ACM 3rd FME Workshop on Formal Methods in Software Engineering. pp. 40–46 (May 2015). https://doi.org/10.1109/FormaliSE.2015.14
5. Jones, A., Kong, Z., Belta, C.: Anomaly detection in cyber-physical systems: A formal methods approach. In: 53rd IEEE Conference on Decision and Control. pp. 848–853 (Dec 2014). https://doi.org/10.1109/CDC.2014.7039487
6. Market, A.: Global cyber-physical system (cps) market by product type and by end-users/application global market share, forecast data, in-depth analysis, and detailed overview, and forecast, 2013 2026. Tech. rep., Apex Market Research (2019)

7. Masci, P., Mallozzi, P., De Angelis, F.L., Serugendo, G.D.M., Curzon, P.: Using PVSio-web and SAPERE for rapid prototyping of user interfaces in Integrated Clinical Environments. In: Verisure2015, Workshop on Verification and Assurance, co-located with CAV2015 (2015)
8. Masci, P., Oladimeji, P., Zhang, Y., Jones, P., Curzon, P., Thimbleby, H.: PVSio-web 2.0: Joining PVS to HCI. In: International Conference on Computer Aided Verification. pp. 470–478. Springer (2015)
9. Owre, S., Rushby, J.M., , Shankar, N.: PVS: A prototype verification system. In: Kapur, D. (ed.) 11th International Conference on Automated Deduction (CADE). Lecture Notes in Artificial Intelligence, vol. 607, pp. 748–752. Springer-Verlag, Saratoga, NY (jun 1992), `http://www.csl.sri.com/papers/cade92-pvs/`
10. Paelke, V., Röcker, C.: User interfaces for cyber-physical systems: Challenges and possible approaches. In: Marcus, A. (ed.) Design, User Experience, and Usability: Design Discourse. Lecture Notes in Computer Science, vol. 9186, pp. 75–85. Springer (2015)
11. Romanovsky, A., Ishikawa, F.: Trustworthy cyber-physical systems engineering. CRC Press (2016)
12. Seshia, S.A., Sadigh, D., Sastry, S.S.: Formal methods for semi-autonomous driving. In: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). pp. 1–5 (June 2015). https://doi.org/10.1145/2744769.2747927
13. Torngreen, M., Bensalem, S., Cengarle, M.V., Chen, D.J., McDermid, J., Passerone, R., Sangiovanni-Vincentelli, A., Runkler, T.: CPS: state of the art. Deliverable D5.1, CyPhERS (Cyber-Physical European Roadmap and Strategy) project (2014)
14. Zheng, X., Julien, C.: Verification and Validation in Cyber Physical Systems: Research Challenges and a Way Forward. In: 2015 IEEE/ACM 1st International Workshop on Software Engineering for Smart Cyber-Physical Systems. pp. 15–18. IEEE (May 2015). https://doi.org/10.1109/SEsCPS.2015.11