Using Co-Simulation to Develop Trustworthy Cyber-Physical Systems

Thomas Roth
National Institute of Standards and Technology[1]
Gaithersburg, MD 20899
thomas.roth@nist.gov

1. Co-Simulation and Trustworthiness of Cyber-Physical Systems

Cyber-physical systems (CPS) are networked systems of humans and devices that both sense and actuate changes on a shared physical space for improved quality of life. Because the control decisions of a CPS will impact the environment and its human occupants, such systems must be protected against both fault and malicious attack. The U.S. National Institute of Standards and Technology (NIST) convened a broad range of experts to support the development of the Framework for Cyber-Physical Systems as a foundation for the discussion of, and reasoning about, CPS [1]. The NIST CPS Framework lists the concerns that may be addressed during the conceptualization, realization, and assurance of CPS or Internet of Things (IoT) systems. These concerns include the trustworthiness aspect which incorporates security, privacy, safety, reliability, and resilience.

One challenge with measuring the trustworthiness of CPS is that many experiments cannot be run on the operational system. Any experiment that results in degraded system performance can have tremendous negative impact on either people or the environment, making it difficult to *stress test* the system under different failure modes. In addition, the geographic scale and cost of CPS make it near impossible to implement an isolated test system. As a result, trustworthiness assessments of CPS often must be done via simulation by necessity.

However, CPS integrate technologies and expertise across multiple domains such as smart cities, smart grid, smart manufacturing, transportation, and others. While each domain has developed simulators tailored to its own requirements, these simulators often do not extend beyond a single domain and are insufficient to create models that reflect the real world behavior of an integrated CPS. For good reasons, the creation and maintenance of a generic *CPS simulator* would be a tremendous undertaking. It would need to support all present and future CPS domains, convince researchers to migrate existing models developed over years of investment, and be usable by users with a vast range of domain expertise. A more desirable approach is to integrate the existing domain specific solutions together to execute a joint simulation. In fact, the integration of multiple simulators, or co-simulation, has been the trend in smart grid research for over a decade [2].

There are two common co-simulation standards. The IEEE 1516-2010 High Level Architecture (HLA) takes a distributed systems approach where the simulators are equal peers in a federation that interact using a common service set [3]. An HLA federation relies on a *runtime infrastructure* (RTI) that implements the common services, and individual simulators must be integrated with the RTI [4]. The U.S. Department of Defense requires HLA support for its models and simulations and this standard is most often used for defense applications and training. The Functional Mock-up Interface (FMI) takes a controller/agent

[1] Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States. Certain commercial products are identified in order to adequately specify the procedure; this does not imply endorsement or recommendation by NIST, nor does it imply that such products are necessarily the best available for the purpose.

approach where the simulators are agents whose execution is controlled by a central co-simulation algorithm [5]. The individual simulators must be packaged into a file called a functional mock-up unit (FMU) that implements a common set of methods invoked by the co-simulation algorithm. FMI is being developed as a Modelica Association Project and has built-in support for several modeling tools.

2. Related Research Activities at NIST

The following describe several NIST activities in co-simulation and trustworthiness:

1. **Develop a portable, open-source software tool to support the co-simulation of complex CPS**.
   NIST, in collaboration with Vanderbilt University, has released and maintained an open-source tool for the development of federated experiments using HLA [6]. One goal of this tool, called the Universal CPS Environment for Federation (UCEF), is to make the development of experiments based on co-simulation more accessible to researchers without extensive background in distributed systems. UCEF allows researchers to design experiments in a graphical modeling language and leverage code generation to transform their models into an executable co-simulation. UCEF was developed to be compliant with strict information technology (IT) security policies, and is available as a self-contained virtual machine with no dependencies on any cloud services. Research at Vanderbilt University using the same software available in UCEF has led to the implementation of a cyber-attack library based on network simulation [7]. This library, combined with a scenario modeling language called Courses of Action, can be used to execute different attack scenarios within a co-simulation such as denial of service or packet manipulation. Current efforts aim to incorporate the cyber-attack library into UCEF.

2. **Demonstrate the use of co-simulation in measuring ADS-Equipped Vehicles safety**.
   NIST hosted a workshop to explore current perspectives across industry, government, and academia on safety requirements and safety measurements for automated driving systems (ADS) [8]. One of the workshop outcomes was identifying community consensus on the need for a comprehensive safety methodology framework to advance the adoption of ADS-equipped vehicle technology. A promising approach to safety measurement is through co-simulation, where the vehicle is simulated in a virtual environment and its trustworthiness is assessed based on its response to a range of scenarios. Initial results at NIST using UCEF demonstrate how co-simulation can be used to assess ADS-equipped vehicle trustworthiness [9].

3. **Develop methods to validate the composition of systems using the NIST CPS Framework**.
   One challenge of CPS is how to handle the reuse of devices and systems. Often a CPS is developed through the composition of existing devices or systems rather than development of entirely new components. This challenge is also prevalent in co-simulation where there might be a library of existing models or simulators that are assembled into a specific experiment configuration. However, there is no guarantee that the final assemblage of functions has no unwanted side effects on overall system trustworthiness or performance. The NIST CPS Framework provides the foundations to develop a common language to describe CPS requirements, and can be used to document or annotate the properties of a CPS [1]. If a composition function is specified using this common language, and the individual systems are documented according to the CPS Framework, then it would be possible to determine the impact of their composition on both trustworthiness and performance of the integrated system based on their documented properties. NIST research activities in this area include developing a *CPS Descriptor* that describes the interfaces and capabilities of a system, developing formal logic to reason about the composition of CPS, and developing a CPS event diagram language that models over time how the cyber/physical/human components cause different impacts on trustworthiness.

3. References

[1] E. Griffor, C. Greer, D. Wollman, and M. Burns, "Framework for cyber-physical systems: Volume 1, overview," 2017, doi: 10.6028/NIST.SP.1500-201.

[2] S. Müller, H. Georg, J. Nutaro, E. Widl, Y. Deng, P. Palensky, M. Awais, M. Chenine, M. Küch, M. Stifter *et al.*, "Interfacing power system and ICT simulators: Challenges, state-of-the-art, and case studies," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 14–24, 2016, doi: 10.1109/TSG.2016.2542824.

[3] "IEEE standard for modeling and simulation (M&S) high level architecture (HLA)– framework and rules," *IEEE Std 1516-2010 (Revision of IEEE Std 1516-2000)*, pp. 1–38, Aug 2010, doi: 10.1109/IEEESTD.2010.5553440.

[4] T. Roth and M. Burns, "A gateway to easily integrate simulation platforms for co-simulation of cyber-physical systems," in *2018 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. IEEE, 2018, pp. 1–6, doi: 10.1109/MSCPES.2018.8405394.

[5] (2014) Functional mock-up interface for model exchange and co-simulation 2.0. [Online]. Available: http://fmi-standard.org

[6] M. Burns, T. Roth, E. Griffor, P. Boynton, J. Sztipanovits, and H. Neema, "Universal CPS environment for federation (UCEF)," in *2018 Winter Simulation Innovation Workshop*, 2018.

[7] H. Neema, B. Potteiger, X. Koutsoukos, G. Karsai, P. Volgyesi, and J. Sztipanovits, "Integrated simulation testbed for security and resilience of CPS," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018, pp. 368–374, doi: 10.1145/3167132.3167173.

[8] E. Griffor, C. Greer, and D. Wollman, "Workshop report: Consensus safety measurement methodologies for automated driving system-equipped vehicles," 2019, doi: https://doi.org/10.6028/NIST.SP.1900-320.

[9] K. Halba, E. Griffor, P. Kamongi, and T. Roth, "Using statistical methods and co-simulation to evaluate ADS-equipped vehicle trustworthiness," in *Electric Vehicles International Conference (EV)*, 2019, pp. 1–5, doi: 10.1109/EV.2019.8892870.