CERES – Thesis proposal #2 on Digital Twin for Building Security Management Systems

Team R3S
SAMOVAR, Télécom SudParis
Institut Polytechnique de Paris

Team ACES
LTCI, Télécom Paris
Institut Polytechnique de Paris

Context

Information systems are increasingly complex and spreading in every sector, often built from off-the-shelf components, with little to no security guarantees whatsoever. In order to regain its sovereignty, a State needs to build its cybersecurity posture from certified software and hardware stacks, security-wise. Testing is thus necessary to assess the level of security of a system but highly reliable on what is and how it is tested. Additionally, testing a real system is not often affordable or feasible for safety reasons. To that end, a certain amount of simulation/emulation is often leveraged to compensate. Recently, the concept of *digital twin* (DT) has been considered to model complex and/or large industrial systems, which safety requirements prevent any direct testing. DT proposes a replica of a complete system by using data related to the state of the system under test, experts knowledge or even data from similar devices. Its usage seems to have found application in industrial systems [1, 4] as it represents a good trade-off between cost and realism, but it is still emerging for complex information systems.

This thesis is part of the CERES project, within the framework of the CIEDS (Interdisciplinary Center for Defense and Security Studies) of Institut Polytechnique de Paris. It is partially funded by the French Agency for Defense Innovation (AID), Ministry of Armed Forces.

Objectives

This thesis aims at supporting the construction of a digital twin platform in a defense-related program. The thesis will study and develop safety and cybersecurity interactions and the modelization of information and physical systems. The resulting platform will enable to run digital twins in a co-simulation mode first, where the heavier physical subsystems are replaced by simulations. In a second stage, the thesis will deepen the interactions between different scientific domains such as IoT and Machine Learning [4] to automate the acquisition and processing of data from heterogeneous sources and feed the digital twin information system. The innovative digital twin approach should be resilient to dynamic changes and able to accommodate the addition of a new component, or the update of existing components, without incurring a complete recomputation of the model.

Proposal

The thesis will study the extensive literature on digital twins that has been produced so far and identifies the potential information gaps. In particular, existing works dealing with safety/cybersecurity aspects will be considered. The thesis aims at leveraging advances in IoT and Machine Learning to extend the DT capacities in terms of sensing and updating the state of the system under test. The innovations will be immediately tested at a small scale on a first prototyping platform of a building information system (a couple of subsystems, at first).

Pending issues in terms of state update will be further investigated in order to understand how to model attacks and their impacts on the DT, and how the DT's updated state will affect, in turn, the test inputs. Recently, model-driven engineering has been a credible candidate to build DTs as they are usually defined in terms of one or more models [3]. It has even been succesfully applied on some industrial use cases, such as *injection molding* [2], but is yet to be applied to building automation. The usage of Machine Learning could complement data collected through IoT probes with mined and/or predicted behavior patterns of a sample of existing or similar systems, at a subsystem level first, and then at a global system-of-systems level. The implications of dependency between modules may represent another typical challenge of update issues. The updated approach will be tested again with a larger prototyping platform.

Finally, the effect of adding remediation actions to the system under test will also be evaluated. While the impact of attacks could be learnt from existing deployments, the reliability of the evaluation of remediations should not be overestimated to ensure fairness.

Application

We are open to applications to be reviewed as soon as possible, and followed by an (remote) interview, if accepted. Potential candidates MUST hold a Master-level degree or equivalent (e.g., a French *diplôme d'ingénieur*) and have experience in domains related to this thesis offer (digital twin, building management systems, machine learning, model-driven engineering) as well as a strong motivation for research. The candidate SHOULD provide the following items as an application package by email to ALL points of contact:

- up-to-date resume (CV);
- a copy of the latest degree (or ongoing if completion date is September 2021);
- letters of recommendation, or a list of references (people that would recommend the candidate).

Incomplete packages will not be reviewed.

Contacts

- Gregory Blanc (`gregory.blanc@telecom-sudparis.eu`)

- Jean Leneutre (jean.leneutre@telecom-paris.fr)
- Olivier Levillain (olivier.levillain@telecom-sudparis.eu)

References

[1] A. Bécue et al. A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future. *Applied Sciences*, 10(13):4482, 2020.

[2] P. Bibow, M. Dalibor, C. Hopmann, B. Mainz, B. Rumpe, D. Schmalzing, M. Schmitz, and A. Wortmann. Model-Driven Development of a Digital Twin for Injection Molding. In *Proc. of CAiSE'20*, pages 85–100. Springer, 2020.

[3] F. Bordeleau, B. Combemale, R. Eramo, M. van den Brand, and M. Wimmer. Towards Model-Driven Digital Twin Engineering: Current Opportunities and Future Challenges. In *Proc. of IC-SMM'20*, 2020.

[4] M.J. Kaur et al. *Digital Twin Technologies and Smart Cities*, chapter The Convergence of Digital Twin, IoT, and Machine Learning: Transforming Data into Action. 2020.