Securing Cyber-Physical Systems through Digital Twins

by Matthias Eckhart (TU Wien) and Andreas Ekelhart (SBA Research)

In recent years, the concept of digital twins has received increasing attention. Virtual replicas of cyber-physical systems (CPSs) can be leveraged for monitoring, visualising and predicting states of CPSs, leading to new possibilities to enhance industrial operations. Yet, the benefit of this concept goes beyond typical Industry 4.0 use cases, such as predictive maintenance. Recent efforts explore how digital twins can increase the security of CPSs.

The adoption of new technologies that follow the Industry 4.0 vision of an interconnected factory significantly increases the attack surface, and thus introduces new attack vectors. Considering that the security of CPSs has a direct impact on safety, implementing adequate security measures is vital. As a result, a holistic security solution that not only protects the CPS during operation, but rather throughout its entire lifecycle is highly desirable. More specifically, such a security solution should aim to (i) support the identification of security weaknesses in the specification, (ii) allow the execution of security and system tests without disrupting physical processes, (iii) monitor the physical process under control, and (iv) detect intrusions and other abnormal conditions of the CPS.

To implement the aforementioned use cases, researchers at TU Wien and SBA Research have been experimenting with the concept of digital twins. While the term "digital twin" typically refers to a data-driven or physical model of a system, we use it to describe an emulated or simulated device that may be connected to an emulated network. In the context of this research, digital twins reflect the correct behaviour of their physical counterparts, as specified by experts from the industrial automation domain. Thus, deviations between the physical device and its digital twin may indicate either malicious behaviour or faults. Furthermore, since the digital twins run in an isolated, virtual environment, they can be analysed in depth without risking the disruption of live systems.

The CPS Twinning framework [1] is an experimental prototype to implement these concepts. As illustrated in Figure 1, the digital twins are generated completely from the specification of the CPS, which consists of artefacts that express engineer and domain knowledge. Ideally, the specification has already been created during the engineering process. Furthermore, security and safety rules (e.g., thresholds for process variables) can be defined in the CPS's specification, providing the means for detecting abnormal conditions in digital twins.

In essence, the proposed digital-twin framework comprises a generator component and a virtual environment. The generator parses the specification in order to create the digital twins in the virtual environment. The virtual environment on the other hand, provides an emulated network stack that the emulated or simulated virtual devices can use for communicating with each other. Moreover, the framework supports two modes of operation, viz. simulation and

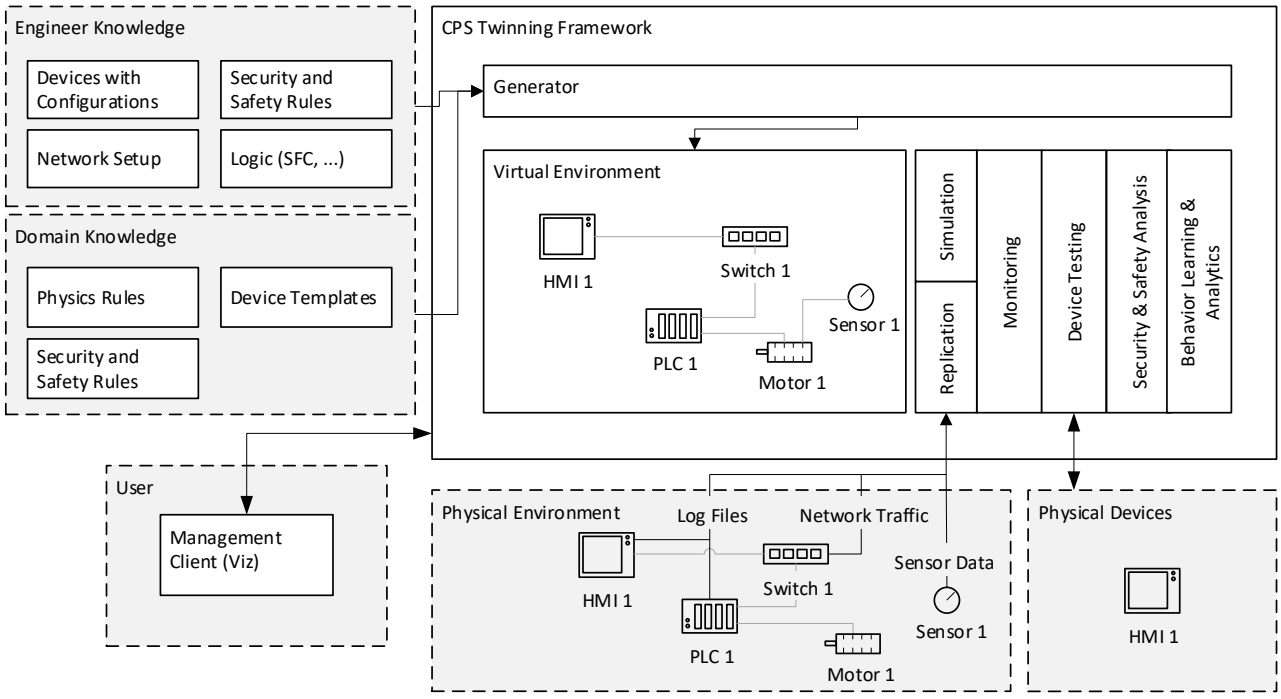

Figure 1: Architecture of CPS Twinning [1], which consists of the generator component, the digital-twin execution environment and modules that implement the use cases.

replication. In simulation mode, the digital twins run independently from their physical counterparts, e.g., to conduct security tests. In contrast, the replication mode mirrors the physical devices' program states to their digital twins. In this mode, malicious behaviour can be detected in two ways: First, a comparison between the inputs and outputs of physical devices and those of digital twins may reveal differences that would indicate malicious behaviour or faults that caused the real devices to deviate from their virtual replicas. Second, if abnormal conditions of the physical process emerge in the virtual environment as well, the framework is able to detect violations of safety and security rules, by continuously monitoring the state of digital twins.

In [1], we present a proof of concept to demonstrate the feasibility of the proposed approach. We used AutomationML [2] as a data format, to specify our exemplary production system. In addition to the CPS's specification, we explicitly defined safety and a security rules. The prototypical implementation of the framework is based on Mininet [3] and integrates a transcompiler for IEC 61131-3 programming languages as well as a Modbus TCP/IP stack. In this way, we were able to equip the digital twins with the required features to replicate the component logic of the physical devices that are part of our test bed.

For future work, we intend to focus on the simulation aspects of digital twins by developing a feature that would allow users to recover historical states of digital twins and replay their execution. In this way, certain scenarios can be repeated for further analysis, e.g., to understand the propagation of malware.

Link:
Source code of CPS Twinning on GitHub: https://kwz.me/hds

References:
[1] M. Eckhart, A. Ekelhart: "Towards Security-Aware Virtual Environments for Digital Twins", Proc. of the 4th ACM Workshop on Cyber-Physical System Security. ACM, 2018.
[2] R. Drath, et al.: "AutomationML-the glue for seamless automation engineering", ETFA 2008.
[3] B. Lantz, B. Heller, N. McKeown: "A network in a laptop: rapid prototyping for software-defined networks", Proc.of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, ACM, 2010.

Please contact:
Matthias Eckhart, TU Wien, Austria
matthias.eckhart@tuwien.ac.at
https://www.sqi.at/

Andreas Ekelhart,
SBA Research, Austria
AEkelhart@sba-research.org
https://www.sba-research.org/

Enabling Security and Safety Evaluation in Industry 4.0 Use Cases with Digital Twins

by Markus Tauber (FH Burgenland) and Christoph Schmittner (AIT)

The digital twin of a system should contain not only the existing information but also an up-to-date picture of the current status. While this is easy with physical properties, which can be measured by sensors, it is more challenging to measure and to provide an up-to-date picture of properties like security and safety. We have investigated the modelling of such dependencies in use cases related to transparency as well as to self-adaptability. Based on our experience we propose further extensions of domains like reliability. This also has the potential to provide legal support to Industry 4.0 use cases when required.

The uptake of technologies and approaches from the Internet of Things (IoT) together with flexible Cloud-based support technologies has enabled numerous and diverse digitisation and Industry 4.0 scenarios and use cases, ranging from smart manufacturing to smart-buildings and smart farming. Each domain has a different environment, and an application must be able to react, i.e. to be smart, to changes in the environment. Such changes need to be monitored and it is important that the application still operates in a trustworthy manner in the face of environmental changes.

Digital twins can help to organise and handle all the data that is generated by IoT elements. Digital twins are a digital representation of a real system, with the history of all changes and developments. Figure 1 gives an overview of how Industry 4.0 is structured and divided between the "real" and the "digital world". The starting point was to have a collection and a standardised digital representation of the real or physical "thing" for easier management. The digital twin is intended as a shell that contains and manages, depending on the application and needs, different sub-models [3].

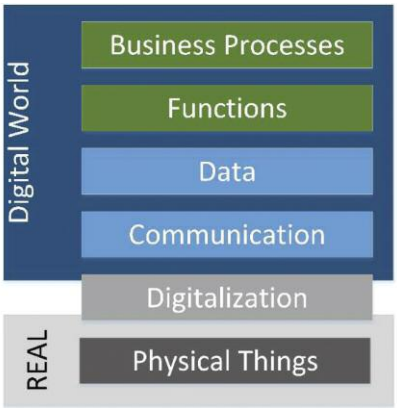

Figure 1: Industry 4.0 Layer-Model.

Although there are already security and safety oriented sub-models based on the IEC 62443 and IEC 61508/61511 these are currently intended as static information. From [1]: "Administration Shell (=digital twin) of Smart Manufacturing Components should be able to carry the