Digital Twins for Cyber-Physical Threat Detection and Response

by Matthias Eckhart, Andreas Ekelhart (SBA Research and University of Vienna), and Roland Eisl (ENRAG)

Since cyber-physical systems are the backbone of smart cities and innovative industrial applications, their safe and secure operation is paramount. However, due to the steadily increasing aggressiveness, sophistication, and stealth of cyberattacks, new methods for threat detection and response are needed. The concept of digital twins opens up new avenues of research to address these gaps.

Recent security incidents involving cyber-physical systems (CPSs), such as the 2021 Colonial Pipeline cyberattack, have again demonstrated the vulnerability of critical infrastructure. While the current state of CPS security is already strained, smart technology trends proceed to evolve, pushing traditional protection mechanisms to their limits. As a result, new methods to support the implementation of a holistic security approach are needed. Considering the interdependency of the cyber and physical domains in which these systems function, adequately protecting CPSs represents a pressing challenge. A few years ago, researchers started to explore how the concept of digital twins can be utilised to tackle this challenge [3].

Within the context of security, the term “digital twin” can be defined as “... a virtual replica of a system that accompanies its physical counterpart during phases of its lifecycle, consumes real-time and historical data if required, and has sufficient fidelity to allow the implementation of the desired security measure.” [3] Since digital twins are not used for redundancy purposes when applied within the context of security, the CPS is virtually replicated by means of emulation, simulation, and modelling techniques to an extent that enables the implementation of security-enhancing features and activities. For example, digital twins that possess a sufficient degree of fidelity allow thorough security testing during both the engineering and the operation phase [1]. This use case of the digital-twin concept spares systems integrators and operators of CPSs the need to build custom testbeds or conduct security tests with the real infrastructure, thereby providing cost savings and preventing uncontrolled interactions with live systems that may lead to extensive (physical) damages. Furthermore, digital twins that run in parallel to their physical counterparts, closely following their states, provide the means to inspect the behaviour of the CPS without the risk of interference. This unique feature allows rigorous monitoring of multiple CPS layers (e.g., physics, network, logic) and can be exploited for detecting intrusions. However, such a security-focused use case necessitates a state replication mechanism to keep the digital twins in sync with their physical counterparts, and further assumes that the virtual replicas exhibit benign behaviour [2]. If an alarm is raised, the digital twins can then be used to identify possible countermeasures and to assess their effectiveness as well as their effects on the physical process from a simulation point of view. As initial efforts were directed toward developing the basic principles of this concept [3], more research is required to efficiently create, operate, and maintain these security-focused digital twins.

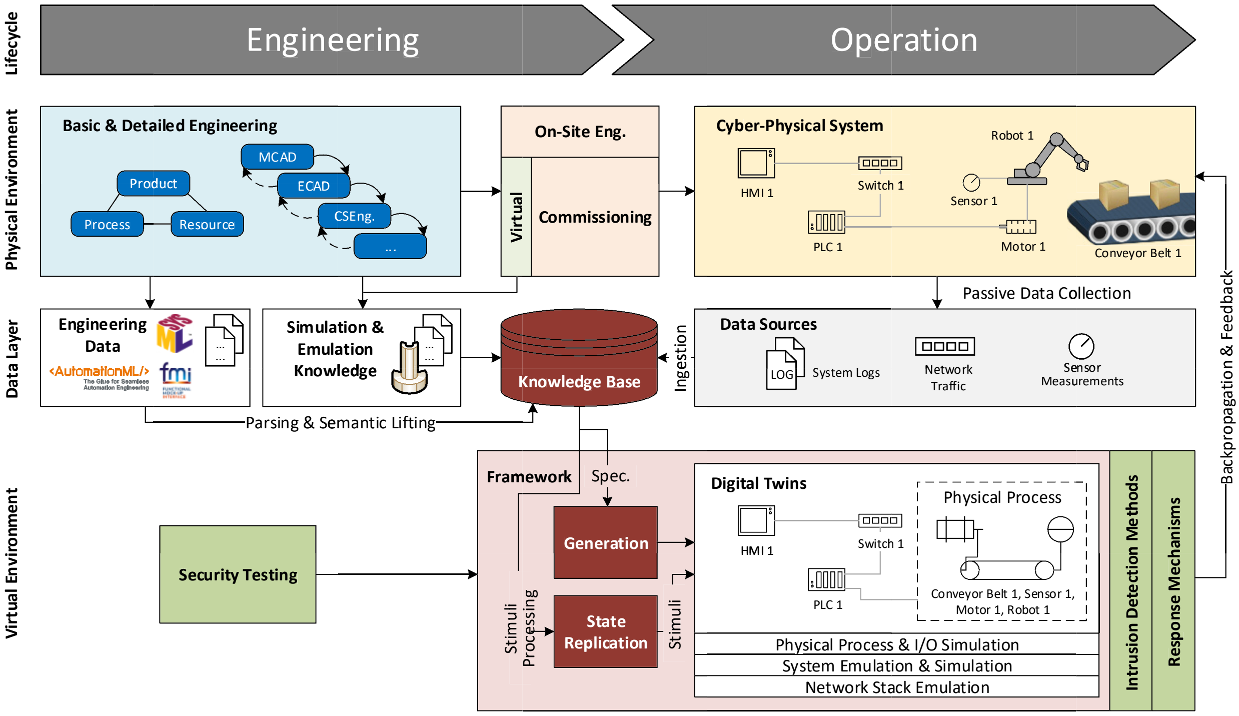

Figure 1: High-level architecture of the digital-twin framework.

The SecurityTwin project [L1] aims to develop the fundamental methods for employing the digital-twin concept to enhance the security of CPSs. As part of this project, researchers at SBA Research and the University of Vienna, together with industry professionals at ENRAG and condignum, will create a framework to efficiently build digital replicas of CPSs based on engineering data, emulating components as well as networks, and simulating physical processes. Figure 1 illustrates the architecture of the digital-twin framework on a high level. We aim to develop a knowledge base that incorporates know-how from numerous heterogeneous data sources (e.g., engineering data repositories, domain knowledge) and provides the semantic foundation for generating the digital twins. This knowledge base comprises: (i) information about the CPS itself (sourced from engineering artifacts); (ii) information concerning the simulation and emulation used as part of the digital twins; and (iii) operational data from the real CPS for state replication and intrusion detection. The digital twins can then be automatically generated by instructing the integrated emulation solutions (e.g., QEMU) and initialising the embedded simulation models. Moreover, a synchronisation mechanism will be developed, which is not only capable of automatically replicating states in a timely manner but also of recovering the digital twins from state mismatches.

Using the architecture we described, our framework will provide the basis for implementing intrusion detection and response methods. Owing to the physical models and simulations integrated into the digital twins, the designed intrusion detection system incorporates knowledge about the physical process under control and thereby will yield alerts if the process is steering toward an unintended state. Upon detection of adverse events, response measures can be identified and their applicability, as well as consequences, assessed by observing the behaviour of the virtual replicas.

Building upon our earlier work [1, 2, 3], we are currently in the process of developing the framework as described above. In addition to our contribution as part of the SecurityTwin project [L1], we want to actively stimulate scientific exchange in this emerging research area. We are therefore organising the Dagstuhl seminar 22171 [L2], which is dedicated to this topic and are encouraging other researchers to share their perspectives.

Links:
[L1] https://kwz.me/h7j
[L2] https://kwz.me/h7q

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] M. Eckhart, A. Ekelhart: "A Specification-based State Replication Approach for Digital Twins", Proc. of the 2018 Workshop on Cyber-Physical Systems Security and Privacy. ACM, 2018.

[3] M. Eckhart, A. Ekelhart: "Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook", Security and Quality in Cyber-Physical Systems Engineering. Springer, 2019.

Please contact:
Matthias Eckhart, Andreas Ekelhart
SBA Research and University of Vienna, Austria
meckhart@sba-research.org,
aekelhart@sba-research.org
https://www.sba-research.org/
https://www.sqi.at/

Roland Eisl
ENRAG, Austria
roland.eisl@enrag.at
https://www.enrag.at/

Circularity and Sustainability in Modern Smart Grids Through Innovative Energy Market Architectures

by Nikolaos Efthymiopoulos, Prodromos Makris, Emmanouel Varvarigos (National Technical University of Athens)

Circularity and sustainability in modern smart grids require open data models that can support dynamic and efficient distribution-network-aware energy management. In this context, the FLEXGRID [L1] project is developing a digital platform that will offer digital energy services (DESs) that help energy sector stakeholders (i.e., Distribution System Operators (DSOs), Transmission System Operators (TSOs), market operators, Renewable Energy Sources (RES) producers, retailers, flexibility aggregators) to: (i) automate and optimise the planning, operation and management of their systems and assets, and (ii) interact in a dynamic and efficient way with the electricity system and other stakeholders.

The large-scale integration of Distributed Energy Resources (DERs), such as PV/wind generation (RES), electric vehicles (EVs), energy storage systems (ESS) and demand side management (DSM) equipment in distribution networks poses new challenges and opportunities for the power sector, as stated in the EU Clean Energy Package [1]. In this context, the FLEXGRID project is investigating the constraints of the current smart grid architecture that prevent large scale DER integration in distribution networks and consequently mitigates circularity and sustainability in modern smart grids.

The first reason is that DSOs use conservative constraints in distributed DER installation to ensure reliable and secure operation of their network. The root cause of this conservatism is the inability of DSOs to dynamically and accurately monitor and manage their networks. The development of a