Digital Twins for Cyber-Physical Threat Detection & Response

Laura Waltersdorfer, Matthias Eckhart, Andreas Ekelhart

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

SBA Research

Problem & Motivation

Cyber-Phyiscal Threats

- **Cyber-Physical Production Systems** (CPPS) are increasingly targeted by tailored threats
- **Malware attacks** can hinder operation, incur safety dangers and cause significant financial damages
- Sophisticated attacks (cf. TRITON [1]) are aimed at **Industrial Control Systems** and show the aggressiveness of such attacks

Security Testing

- Security testing in CPPS is inherently difficult due to the following reasons:
  (i) high costs for **custom infrastructure of testbeds**
  (ii) simulation of systems **highly complex**
  iii) **space constraints**
- Past attempts to perform penetration testing on CPPSs demonstrated **critical malfunctions**, uncontrolled disruption of operation and significant potential danger to human workers [2]

Detecting Cyber Threats with Digital Twins

Digital Twin Generation & Usage

- Digital Twins, virtual replicas of the CPPS, can be generated based on artefacts and engineering data (e.g. AutomationML files) in a cost-efficient way for security use cases [4]
- The real-system behavior is reflected in the digital twin, for example by passive state replication as shown in [3]
- The virtualisation enables the monitoring of the system according to process logic, assuring the adherence of specified states, comparing data and testing of future adaptations in a virtual, realistic environment

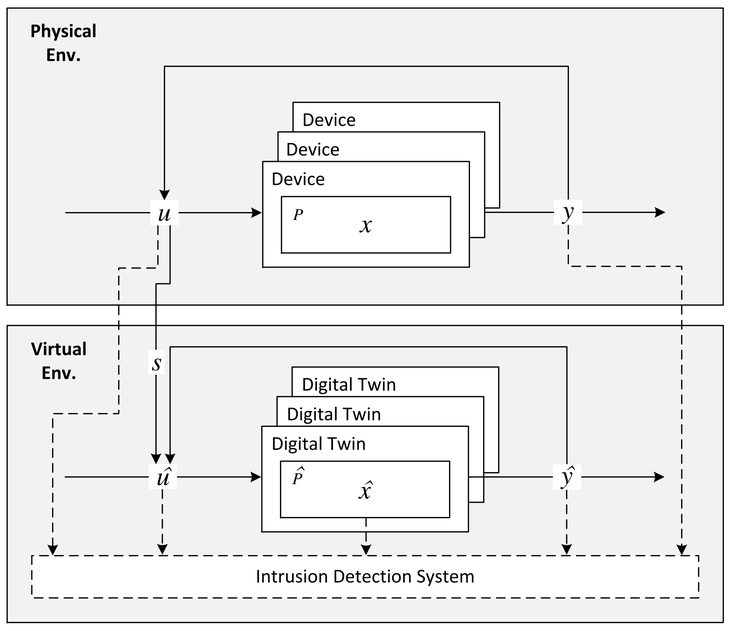

Figure 1: State Replication [3]

Advanced Security Use Cases for Digital Twins

Intrusion Detection

- The multi-dimensional nature of production processes must be addressed: process level (i.e. physics level), sensing and manipulation (e.g. PLC logic, sensor data and network level)
- Anomalies can be detected based on the specified behavior and provided safety rules

Response & Reconfiguration

- Proactive and reactive responses can be incorporated in the Digital Twin to increase resilience of CPPS

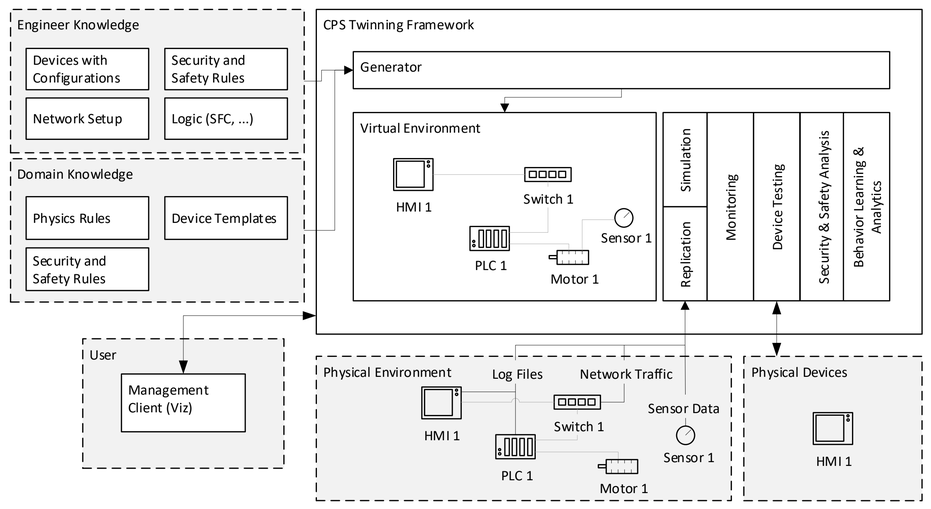

Figure 2: Digital Twin Framework Architecture

Conclusion

- Automatic generation of Digital Twins based on artefacts and engineering data is a cost-effective and low-effort measure to create an **enhanced security testing environment** for CPPS
- Digital Twins can help to increase the **security testing capabilities** under otherwise challenging circumstances and enable experts to play out different scenarios in the production system domain **without disturbing operation**

Future Work

- Behavior specification-based Intrusion Detection Systems seem promising for industrial systems to detect threats
- Integration of semi-automated deployment of reconfiguration **can increase the resilience of CPPS**

[1] AC Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems. In Proc. Black Hat USA, pages 1–26, 2018.
[2] David Duggan, Michael Berg, John Dillinger, and Jason Stamp. Penetration testing of industrial control systems. Sandia national laboratories, 2005.
[3] Matthias Eckhart and Andreas Ekelhart. A specification-based state replication approach for digital twins. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, pages 36–47, 2018.
[4] Matthias Eckhart and Andreas Ekelhart. Towards security-aware virtual environments for digital twins. In Proceedings of the 4th ACM workshop on cyber-physical system security, pages 61–72, 2018.

This research was further funded by the FFG under the industrial PhD program (grant no. 874644). Moreover, the financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development is gratefully acknowledged.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.