Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins

Matthias Eckhart, Andreas Ekelhart, and Edgar Weippl

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

Background & Motivation

Cyber Situational Awareness refers to what an individual is aware of regarding events (e.g., issues, attack attempts) that occur in the cyber domain (e.g., networks) [6].

This state can be achieved at different levels [5]:

- Perception,
- Comprehension, and
- Projection of a situation.

Necessary for proper incident handling (e.g., understanding the anatomy of cyber attacks).

Problems

- Learning about incidents may be limited to the use of passive data collection approaches (active techniques may negatively affect the real-time performance).
- CPSs have stringent availability requirements (cannot be simply put out of operation for inspection).
- Difficult to retain valuable information for analysis.

Need: Ability to passively observe the state of CPSs without negatively affecting their operation.

A Cyber Situational Awareness Framework Based on Digital Twins

Contribution [4]: Improves cyber situational awareness by means of visualization and replaying recorded states from real devices to digital twins to reproduce events.

Overview

- Digital twins refer to simulated or emulated devices (e.g., PLCs, HMIs, sensors) that are connected to an emulated network [1, 3].
- Digital twins can be automatically generated from the specification of the CPS [2].
- We extend the open-source framework CPS Twinning: `https://github.com/sbaresearch/cps-twinning`
- Program states are passively mirrored from real devices to digital twins.
- Program and network layer of digital twins can be easily monitored.

Visualization

- Framework provides visualization panel that illustrates the CPS's topology.
- The digital twins' program variables can be monitored in real-time.
- Planned: visual feedback for user-defined alarms, detected intrusions and security metrics.

Record & Replay

- State replication [1] causes stimuli to be directly streamed to the digital twins (limits analysis capabilities).
- Framework stores stimuli for the purpose of replicating them at a later time.
- Users can step back or move forward in the state timeline of digital twins.
- Allows to easily inspect past behavior and establishes a reproducible analysis process.

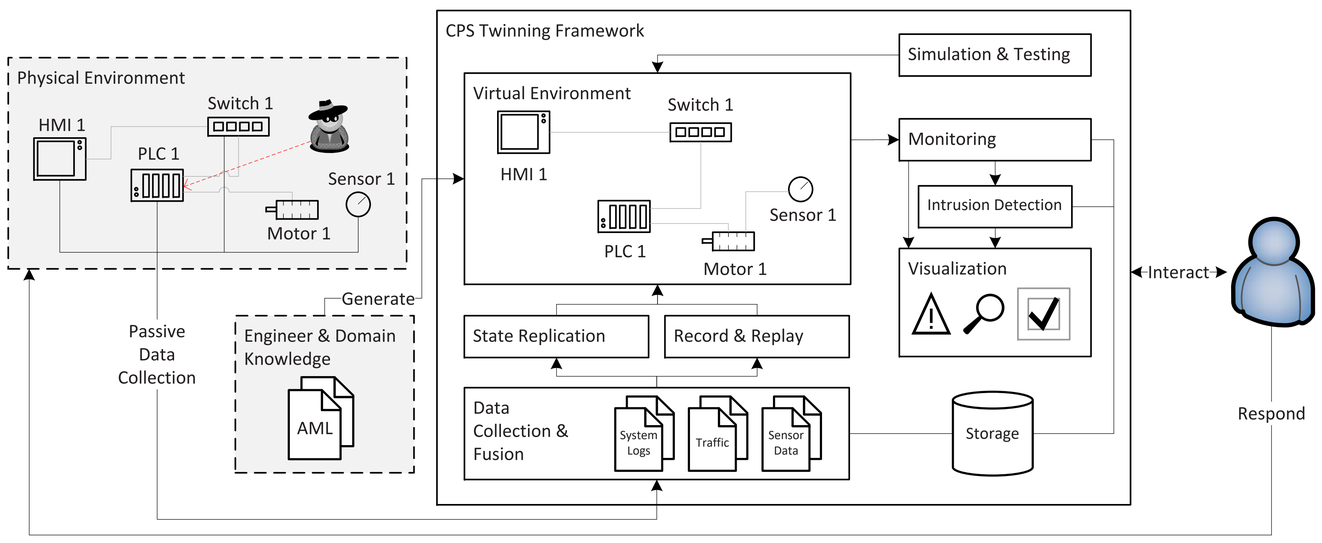

Figure 1: The architecture of the proposed digital-twin cyber situational awareness framework.

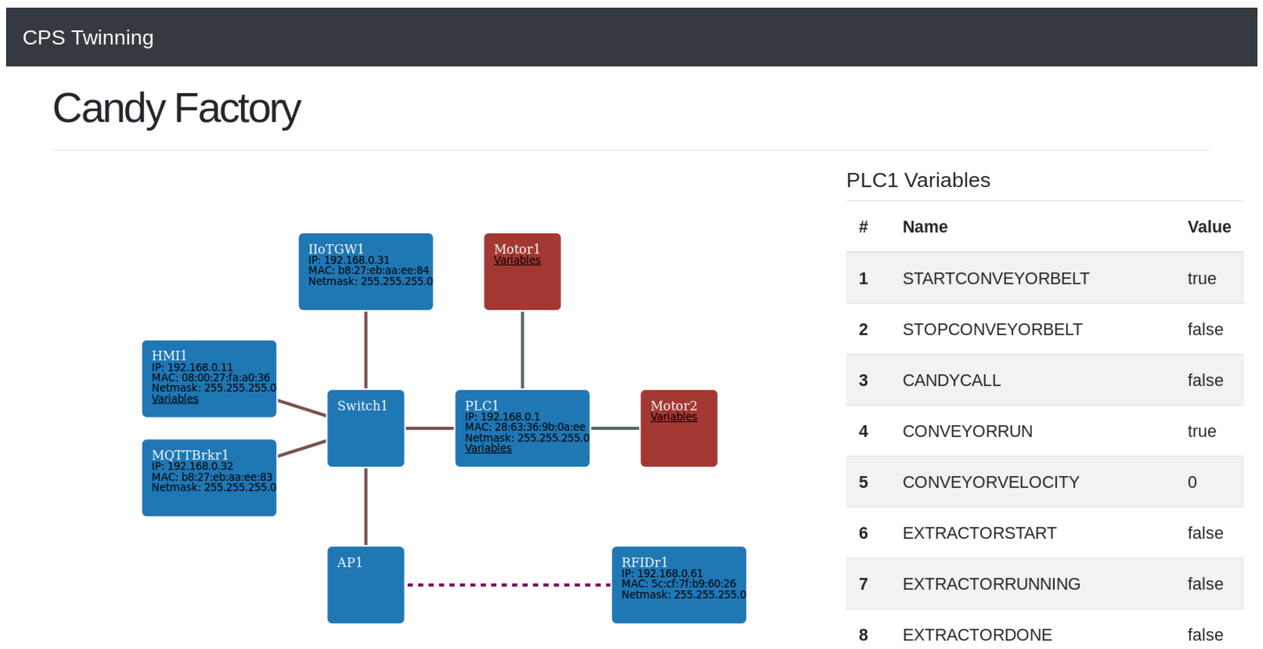

Figure 2: The visualization of digital twins, depicting the CPS's topology and program variables of (virtual) devices.

Use Cases

- **Risk Assessment:** Simulate threat scenarios and assess their impact.
- **Monitoring:** Indirectly observe the system behavior via digital twins.
- **Incident Handling:** Elucidate cyber incidents by means of visual analytics and the record-and-replay feature.

Conclusion

- Provides advanced monitoring, inspection, and testing capabilities.
- Based on the digital-twin framework CPS Twinning [2, 1].
- Further development required for improving visualizations and completing the record-and-replay feature.

[1] M. Eckhart and A. Ekelhart. A specification-based state replication approach for digital twins. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, CPS-SPC '18, pages 36–47, New York, NY, USA, 2018. ACM.
[2] M. Eckhart and A. Ekelhart. Towards security-aware virtual environments for digital twins. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, CPSS '18, pages 61–72, New York, NY, USA, 2018. ACM.
[3] M. Eckhart and A. Ekelhart. Digital twins for cyber-physical systems security: State of the art and outlook. In Stefan Biffl, Matthias Eckhart, Arndt Lüder, and Edgar Weippl, editors, *Security and Quality in Cyber-Physical Systems Engineering*, volume 1. Springer International Publishing, 2019.
[4] M. Eckhart, A. Ekelhart, and E. Weippl. Enhancing cyber situational awareness for cyber-physical systems through digital twins. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1222–1225, Sep. 2019.
[5] M. R. Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1):32–64, 1995.
[6] U. Franke and J. Brynielsson. Cyber situational awareness – a systematic review of the literature. *Computers & Security*, 46:18 – 31, 2014.

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.