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

Matthias Eckhart*†, Andreas Ekelhart*†, Edgar Weippl*†
*Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle, TU Wien, Vienna, Austria
†SBA Research, Vienna, Austria
{matthias.eckhart, edgar.weippl}@tuwien.ac.at, andreas.ekelhart@sba-research.org

***Abstract*—Operators of cyber-physical systems (CPSs) need to maintain awareness of the cyber situation in order to be able to adequately address potential issues in a timely manner. For instance, detecting early symptoms of cyber attacks may speed up the incident response process and mitigate consequences of attacks (e.g., business interruption, safety hazards). However, attaining a full understanding of the cyber situation may be challenging, given the complexity of CPSs and the ever-changing threat landscape. In particular, CPSs typically need to be continuously operational, may be sensitive to active scanning, and often provide only limited in-depth analysis capabilities. To address these challenges, we propose to utilize the concept of digital twins for enhancing cyber situational awareness. Digital twins, i.e., virtual replicas of systems, can run in parallel to their physical counterparts and allow deep inspection of their behavior without the risk of disrupting operational technology services. This paper reports our work in progress to develop a cyber situational awareness framework based on digital twins that provides a profound, holistic, and current view on the cyber situation that CPSs are in. More specifically, we present a prototype that provides real-time visualization features (i.e., system topology, program variables of devices) and enables a thorough, repeatable investigation process on a logic and network level. A brief explanation of technological use cases and outlook on future development efforts completes this work.**

***Index Terms*—Digital twins, cyber situational awareness, information security, cyber-physical systems, cyber defense**

I. Introduction

Cyber-physical systems (CPSs) are considered as disruptive technologies that have the potential to transform entire sectors (e.g., manufacturing), given their integrated nature that fuses computational and physical elements [1]. Considering their increased connectivity capabilities, which may open up new attack vectors, and the fact that security incidents can lead to safety issues, these systems must be adequately protected against adversaries throughout their entire lifecycle. Implementing such a holistic security concept evidently requires a thorough understanding of the CPSs themselves within each lifecycle phase (e.g., plant operation) and the cyber threats that may come into existence. However, the CPSs' key characteristics (e.g., advanced connectivity, dynamic and self-adaptive in nature) also entail complexity that security professionals need to cope with. The issue of high complexity inherent to these systems is aggravated by the fact that the CPS and, in particular, the industrial control system (ICS) threat landscape is extensive and continuously evolving (cf., for instance, [2]), possibly leading to a poor comprehension of the cyber situation.

According to Franke and Brynielsson [3], 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., industrial networks). Following the general definition of situation(al) awareness proposed by Endsley [4], this state can be achieved to different levels, viz., the (i) perception, (ii) comprehension, and (iii) projection of a situation. On the technological side, cyber situational awareness involves data collection, processing, and fusion, leading to systems that aim to provide decision support [3]. Understanding the anatomy of cyber attacks in order to ensure proper incident handling is just one of the reasons why cyber situational awareness is worthwhile. However, providing effective support for cyber situational awareness is difficult [5], especially since the CPS domain presents significant new challenges that need to be overcome. In particular, obtaining events regarding CPSs may be limited to the use of passive data collection approaches, since active techniques may negatively affect the real-time performance. As these systems typically also have stringent availability requirements and may store valuable information in volatile memory (e.g., parameterization), they cannot be simply put out of operation to perform a quick analysis.

The herein proposed cyber situational framework aims to address these challenges. This work builds upon and extends our previous research on leveraging the digital-twin concept for securing CPSs (cf. [6]–[9]). More specifically, we extend *CPS Twinning*[1] [6], i.e., a framework that provides an execution environment for digital twins, which can be automatically generated from the CPS's specification. In the context of this framework, a digital twin refers to a simulated or emulated device, such as a programmable logic controller (PLC), that is connected to an emulated network [7]. The novel contribution

The COMET center SBA Research (SBA-K1) is funded within the framework of COMET — Competence Centers for Excellent Technologies by BMVIT, BMDW, and the federal state of Vienna, managed by the FFG. 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.

[1] https://github.com/sbaresearch/cps-twinning

978-1-7281-0303-7/19/$31.00 ©2019 IEEE

of this research is to show how digital twins can improve the cyber situational awareness regarding CPSs, by means of visualization and replaying recorded states of digital twins for reproducing certain events in a timely manner. In this paper, we share our early experiences of developing the cyber situational framework and describe plans for further research.

The remainder of this paper is structured as follows. Section II discusses related work in the areas of cyber situational awareness and digital twins in the context of information security. After that, we present in Section III the main contribution of this paper, i.e., our novel digital-twin-powered cyber situational awareness framework. In Section IV, we discuss potential use cases of the framework. Finally, Section V concludes the paper and outlines our plans for further development.

II. Related Work & Background

Before presenting our work in progress, we briefly review selected publications that introduce methods for improving cyber situational awareness in the context of CPSs. Furthermore, we explain our previous research on utilizing the digital-twin concept for securing CPSs to set the stage for Section III.

A. Cyber Situational Awareness

A considerable amount of literature has been published on improving cyber situational awareness for CPSs or, more specifically, ICSs [3]. Much of this literature pays particular attention to critical infrastructures, such as power grids [3]. Furthermore, we observed that works in this area touch on various aspects of the cyber situational awareness spectrum.

For instance, in [10] the authors present three correlation methods that can be put to use for identifying similarities among security-relevant documents (e.g., security advisories). The identified relationships among these documents may not only aid administrators in assessing the impact of security events (e.g., incidents) but also support the mitigation process.

Another line of research focuses on the development of metrics and visualization techniques. For example, Matuszak et al. [11] present a visualization framework that is based on multiple metrics that indicate how trustworthy a node of a smart grid system is. As the authors state, the trust visualizations may allow operators to identify compromised nodes and, thereafter, remove them from the smart grid. The authors demonstrate the effectiveness of their implemented framework by providing screenshots of visual feedback that was received during attack simulation.

Besides information correlation and visualization, a plethora of papers have been published in other research areas discussing techniques that aim to improve cyber situational awareness [3]. However, a careful study of the literature did not reveal any previous works investigating how the digital-twin concept can be applied in this context.

B. CPS Twinning

As already indicated, we introduced a digital-twin framework named *CPS Twinning*[1] in our earlier works [6]–[8]. This framework enables users to automatically generate digital twins from the CPS's specification, which may exist in the form of AutomationML-based engineering artifacts [6]. The digital twins are executed within a virtual environment and can run either independently from their physical counterparts (e.g., for testing purposes) or closely follow their program states in order to virtually replicate the behavior of the real CPS on the logic and network layer [7] (e.g., for monitoring purposes). Although the digital-twin concept gives rise to a multitude of security-enhancing use cases [9], we put special emphasis on the development of intrusion detection systems (IDSs). In particular, we implemented a knowledge- [6] and behavior-specification-based IDS [7] based on this framework. Both intrusion detection approaches will also be a building block of the herein presented cyber situational framework, as they alert administrators about any malicious activity.

III. A Cyber Situational Awareness Framework Based on Digital Twins

The framework was designed with the objective of improving cyber defense capabilities of CPSs operators. Operations staff need accurate cyber situational awareness, as they have to be ready to intervene in the face of cyber threats for being able to rapidly adapt security measures. We argue that this requires simulations with sufficient fidelity that can be fed with operational data collected from real devices, which goes far beyond common network security monitoring. In the following, we report on the implementation progress toward this end. The developed prototype is open source and can be found on GitHub[1].

A. Overview

As can be seen in Fig. 1, the virtual environment, which hosts the digital twins, lies at the heart of the proposed framework. Data (e.g., system logs, network traffic, sensor measurements) is passively collected from the physical environment to mirror the program states of real devices to digital twins (cf. [7]). Based on this state replication mechanism, the behavior of digital twins can be monitored on the program and network layer and potential intrusions can be detected. Note that the digital twins should exhibit the correct, benign behavior of their physical counterparts, due to the fact that they are generated from the CPS's specification. However, it is important to understand that the digital twins do not necessarily reflect the actual behavior of real devices. Yet this, in turn, allows to spot deviations that could indicate malicious activity. On the other hand, if vulnerabilities or errors in the specification exist, the digital twins may exhibit malicious behavior similar to their physical counterparts. Additional monitoring or intrusion detection rules can be put in place to remedy this issue.

The beauty of the proposed framework is that the digital twins provide sufficient fidelity to advance cyber situational awareness. Implementation-wise, the prototype is based on Mininet-WiFi [12] and provides the means to execute IEC 61131-3 code in the context of digital twins (cf. [6], [7]). As

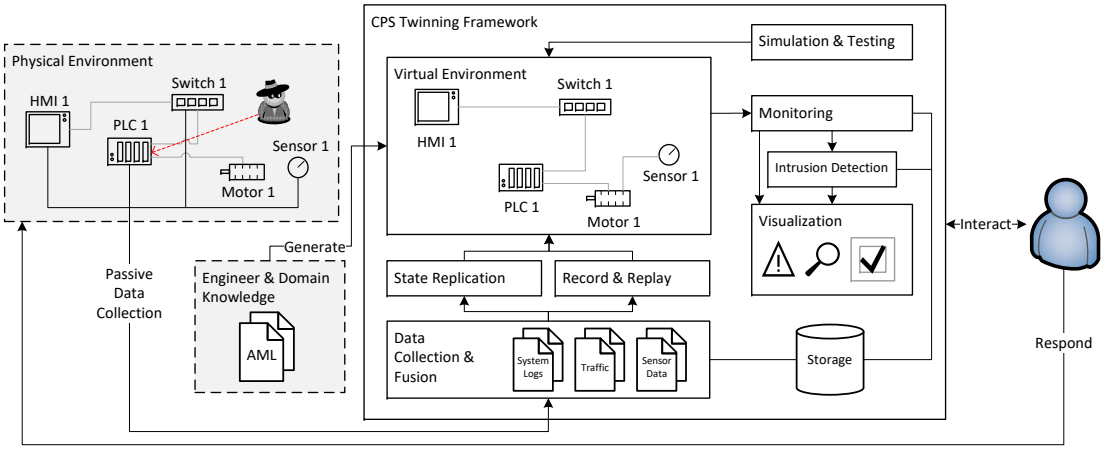

Fig. 1. The architecture of the proposed digital-twin cyber situational awareness framework.

a result, the functionality of devices (i.e., programs, network communication) can be emulated or simulated. The achieved fidelity of digital twins represents a crucial element in the context of cyber situational awareness, since more accurate virtual replicas provide better inspection capabilities. We leveraged this property in the design of the two key components for improving cyber situational awareness, viz., the visualization, and the record-and-replay feature.

B. Visualization

According to Franke and Brynielsson [3], there is a consensus in the community on the importance of visualization for cyber situational awareness. Following this conception, we put emphasis on designing effective visualizations that convey security-relevant information and thereby support the decision-making process. Fig. 2 depicts the preliminary results of this undertaking. This screenshot shows the web page of the visual analytics panel in CPS Twinning with an exemplary scenario (candy factory testbed [7]). The main area of this page contains a graph for the visualization of the CPS's topology, which has been developed with cola.js[2]. Each node in this graph represents a digital twin and the edges are drawn as per the physical network defined in the specification. Furthermore, the connection type is indicated by the line color (e.g., brown: wired network link, green: wired I/O) and pattern (e.g., dashed line: wireless link). As part of each node, the digital twins' connectivity information (i.e., IP address, netmask, MAC address) is displayed so that network issues can be addressed promptly if necessary. In addition, users can select a digital twin on the graph to monitor its program variables, as can be seen on the right side of Fig. 2. Program variable changes are reflected in real-time and highlighted in yellow to draw the user's attention to these events.

As a next step, we plan to improve the visualizations by adding visual feedback for user-defined alarms, detected intrusions and security metrics. Moreover, we aim to extend the graph in a way that the zones and conduits, and the network segmentation is considered in the topology visualization.

[2]https://ialab.it.monash.edu/webcola

C. Record & Replay

In [7], we introduced a specification-based state replication approach that allows to mirror stimuli (i.e., the roots of inputs to devices) from the physical to the virtual environment. This state replication mechanism ensures that the digital twins continuously follow the program states of their physical counterparts. In this way, users can monitor and inspect the digital twins as they transition from state to state. However, if this mode of CPS Twinning is active, the stimuli are directly streamed to the digital twins, limiting the framework's analysis capabilities in terms of inspecting past behavior. To overcome this limitation, we propose a record-and-replay feature that stores stimuli for the purpose of replicating them at a later time. This feature provides the means to establish a reproducible analysis process, since users can restore historical states of digital twins as desired. Stepping back or moving forward in the state timeline of digital twins enables a repeatable, in-depth analysis of certain scenarios and may thereby further improve cyber situational awareness.

Although we can already report preliminary results, the record-and-replay feature is still in development. In particular, dealing with state mismatches caused by an inconsistent initial state (i.e., digital twins have to be reset accordingly) represents a challenging issue that needs to be resolved.

IV. Use Cases

In this section, we provide technical use cases that aim to illustrate the added value of the proposed digital-twin framework for improving cyber situational awareness for CPSs.

a) Risk Assessment: Simulating threat scenarios and assessing their potential impact, by means of the framework's record-and-replay feature, may support situation comprehension and projection. In this way, users may be able to assess

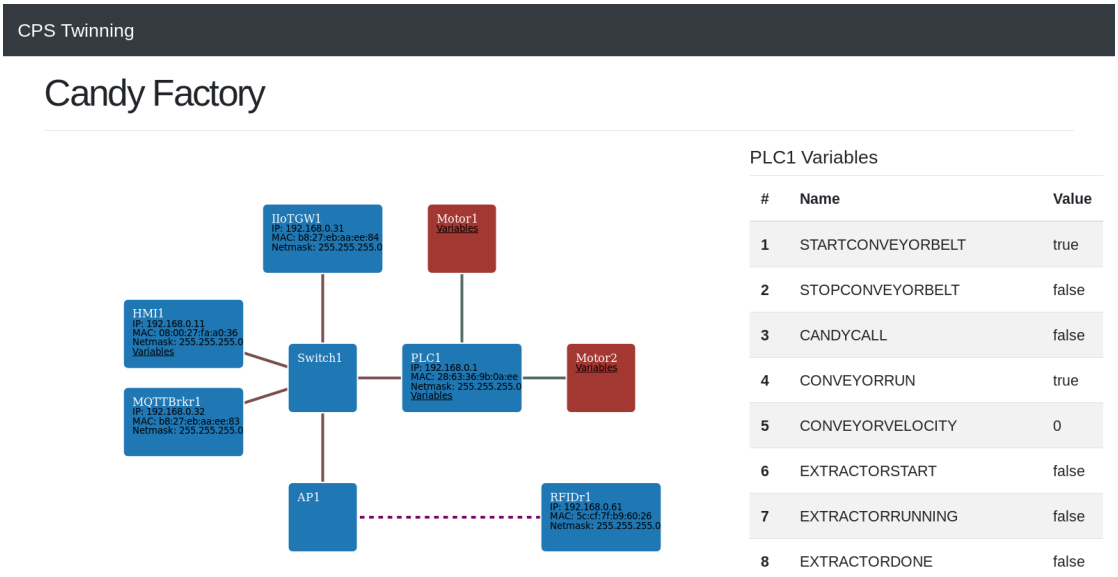

Fig. 2. The visualization of digital twins, depicting the CPS's topology and program variables of (virtual) devices.

the risk of certain attack vectors and can adapt and simulate cyber-defense measures accordingly.

b) Monitoring: Users can indirectly observe the system behavior via digital twins, either by means of the visualization feature or the virtual environment. Moreover, the IDS [6], [7] alerts them if suspicious activity has been detected. As the monitoring and intrusion detection capabilities provide pointers to devices under attack, the framework supports the operations staff in mitigating intrusions and their effects.

c) Incident Handling: Comprehending the current situation is essential for taking appropriate incident response actions. Besides visual analytics to quickly spot issues, the record-and-replay feature of the framework can help in elucidating cyber incidents. For example, stopping the digital twins at certain points for inspection, and recovering past states, may allow users to understand the evolution of a situation. Thereby, users can analyze the situation in depth, from the source of attacks up to the incident taking place and the consequences thereof.

V. Conclusion

In this paper, we have presented our work in progress toward the development of a digital-twin cyber situational awareness framework for CPSs. This framework leverages the concept of digital twins to provide advanced monitoring, inspection, and testing capabilities. The introduced technical use cases illustrate how these features support operations staff in gaining situation perception, comprehension, and projection. Further development effort is required to improve the visualization of digital twins and to bring the record-and-replay feature to completion. Ideally, in the future, the introduced concept could be taken even one step further: instead of providing only decision support, the digital-twin framework could automate the detection and mitigation of vulnerabilities, similar to a cyber reasoning system.

References

[1] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology*, vol. 12, pp. 161–166, 2011.

[2] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016.

[3] U. Franke and J. Brynielsson, "Cyber situational awareness a systematic review of the literature," *Computers & Security*, vol. 46, pp. 18 – 31, 2014.

[4] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[5] M. R. Endsley and E. S. Connors, "Foundation and challenges," in *Cyber Defense and Situational Awareness*, A. Kott, C. Wang, and R. F. Erbacher, Eds., vol. 1. Springer International Publishing, 2014, pp. 7–27.

[6] 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*, ser. CPSS '18. New York, NY, USA: ACM, 2018, pp. 61–72.

[7] ——, "A specification-based state replication approach for digital twins," in *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, ser. CPS-SPC '18. New York, NY, USA: ACM, 2018, pp. 36–47.

[8] ——, "Securing cyber-physical systems through digital twins," *ERCIM News*, vol. 2018, no. 115, 2018. [Online]. Available: https://ercim-news.ercim.eu/en115/special/2101-securing-cyber-physical-systems-through-digital-twins

[9] ——, "Digital twins for cyber-physical systems security: State of the art and outlook," in *Security and Quality in Cyber-Physical Systems Engineering*, S. Biffl, M. Eckhart, A. Lüder, and E. Weippl, Eds., vol. 1. Springer International Publishing, 2019.

[10] G. Settanni, Y. Shovgenya, F. Skopik, R. Graf, M. Wurzenberger, and R. Fiedler, "Correlating cyber incident information to establish situational awareness in critical infrastructures," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec 2016, pp. 78–81.

[11] W. J. Matuszak, L. DiPippo, and Y. L. Sun, "Cybersave: Situational awareness visualization for cyber security of smart grid systems," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 25–32.

[12] R. R. Fontes, S. Afzal, S. H. B. Brito, M. A. S. Santos, and C. E. Rothenberg, "Mininet-wifi: Emulating software-defined wireless networks," in *2015 11th International Conference on Network and Service Management (CNSM)*, Nov 2015, pp. 384–389.