

Digital Twins for Cyber-Physical Systems Security

Alvaro Cárdenas Mora^{*1}, Simin Nadjm-Tehrani^{*2}, Edgar Weippl^{*3},
and Matthias Eckhart^{†4}

1 University of California – Santa Cruz, US. alacarde@ucsc.edu

2 Linköping University, SE. simin.nadjm-tehrani@liu.se

3 Universität Wien, AT. edgar.weippl@univie.ac.at

4 SBA Research – Wien, AT. meckhart@sba-research.org

Abstract

Cyber-physical systems (CPSs) may constitute an attractive attack target due to the increased networking of components that yields an expanded attack surface. If their physical control capabilities are compromised, safety implications may arise. Thus, it is vital that the CPSs being engineered are thoroughly tested and that adequate response measures can be realized upon detecting intruders during operation. However, security testing is hard to conduct due to expensive hardware, limited maintenance periods, and safety risks. Furthermore, the increased stealthiness of threat actors requires new intrusion detection and response methods. Interestingly, digital twins have become an important concept in industrial informatics to solve similar problems, yet with a non-security-related focus: Digital twins that virtually replicate the real systems provide cost-efficient modeling, testing, monitoring, and even predictive capabilities. However, until recently, the digital-twin concept has mainly focused on production optimizations or design improvements without considering its potential for CPS security. The Dagstuhl Seminar 22171 “Digital Twins for Cyber-Physical Systems Security” therefore aimed to serve as an interdisciplinary, open knowledge-sharing platform to investigate the benefits and challenges of applying the digital-twin concept to improve the security of CPSs.

Seminar April 24–29, 2022 – <http://www.dagstuhl.de/22171>

2012 ACM Subject Classification Security and privacy → Intrusion/anomaly detection and malware mitigation; Computer systems organization → Embedded and cyber-physical systems

Keywords and phrases cyber-physical systems, digital twins, information security, production systems engineering, SCADA, industrial control systems, Industry 4.0

Digital Object Identifier 10.4230/DagRep.12.4.54


1 Executive Summary

Matthias Eckhart (SBA Research – Wien, AT, meckhart@sba-research.org)

Alvaro Cárdenas Mora (University of California – Santa Cruz, US, alacarde@ucsc.edu)

Simin Nadjm-Tehrani (Linköping University, SE, simin.nadjm-tehrani@liu.se)

Edgar Weippl (University of Vienna & SBA Research – Wien, AT, edgar.weippl@univie.ac.at)

License  Creative Commons BY 4.0 International license

© Matthias Eckhart, Alvaro Cárdenas Mora, Simin Nadjm-Tehrani, Edgar Weippl

In the light of the increasing digitization and move toward Industry 4.0 [1], cyber security becomes more and more important for cyber-physical systems (CPSs). The advanced computation, communication, and control capabilities of CPSs lead to a wider attack surface and greater exposure to security flaws. Furthermore, the added complexity puts

* Editor / Organizer

† Editorial Assistant / Collector



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 4.0 International license

Digital Twins for Cyber-Physical Systems Security, *Dagstuhl Reports*, Vol. 12, Issue 4, pp. 54–71

Editors: Matthias Eckhart, Alvaro Cárdenas Mora, Simin Nadjm-Tehrani, and Edgar Weippl



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

a considerable burden on security professionals, who have to ensure that the CPSs are adequately protected against adversaries throughout the entire lifecycle. As a matter of fact, designing holistic security measures is a significant ongoing challenge for academia and industry alike. Thorough security testing during the engineering- and, particularly, the operation phase is often not feasible. The development of custom CPS testbeds is complicated, expensive, and time-consuming due to high hardware costs, space constraints, and complex dependencies between components [2]. Past attempts to conduct penetration tests directly on live systems led to unintended system behavior, putting human workers in significant danger and causing a disruption of production lines [3]. In addition to regular security testing, adequate countermeasures need to be implemented in response to newly discovered vulnerabilities that emerge during operation or if the CPS is already under attack. However, the steadily increasing sophistication of cyberattacks calls for more effective intrusion detection and prevention techniques. On top of that, new mechanisms to test and evaluate attack response strategies in a controlled setting are required.

A digital twin, that is, a virtual replica of a real system, was originally envisioned for similar, yet non-security-related purposes: The life of a spacecraft is virtually mirrored through high-fidelity simulations and sensor updates to detect anomalies and safely test mitigation options such that degradation can be reduced and damages prevented [4]. This idea was picked up by the industrial informatics community, whose members implemented the digital-twin concept in various CPS applications for monitoring, lifecycle management, and decision support [5, 6, 7]. In the past few years, researchers have also shown interest in utilizing digital twins for security-enhancing purposes [8, 9, 10, 11, 12, 13]. Although the definition of what constitutes a digital twin in the context of cybersecurity differs in the literature, its main application areas seem to be clear: Virtually replicated systems by means of emulation, simulation, and modeling technologies, coupled with real-time or historical data flows, might be used to improve security testing, intrusion detection, and attack recovery. However, fundamental research questions and challenges remain before digital twins can be applied for security-enhancing purposes. Furthermore, concerns have been raised about the potential security threats associated with the digital-twin concept [14].

Thus, the primary goal of this Dagstuhl Seminar was to lay the foundation for future interdisciplinary collaboration on digital-twin research for CPS security. The interdisciplinary character of this novel research area is reflected in its origin. As already indicated, the notion of using “twins” originally emerged from the space industry [6], gained wider adoption by the industrial informatics community [5, 6, 7], and was eventually applied with the objective of attaining security improvements [8, 9, 10, 11, 12, 13]. For this reason, the seminar has brought together 20 researchers with backgrounds in computer security, control theory, automation engineering, and data science. Inspired by the concept’s promised security improvement potential, the seminar was structured along three different themes:

Foundations of Security-focused Digital Twins. This theme was motivated by the lack of clarity around the digital-twin concept. Therefore, the purpose of this theme was to develop a common understanding of what a digital twin in the context of security is, how it can be defined, and how it relates to existing concepts, such as cyber ranges, data-driven models, and honeypots. Closely tied to this theme were discussions on methods for digital-twin implementation, including (i) emulating systems and simulating physical processes, (ii) knowledge retrieval for digital-twin generation in greenfield and brownfield environments, and (iii) synchronizing digital twins with their physical counterparts.

Intrusion Detection. The objective of this theme was to explore intrusion detection as a potential use case for digital twins. Assuming that the digital twin is built from a benign specification such that legitimate behavior is exhibited when executed in sync with its counterpart, any deviations observed on the logic, network, and physics layers could indicate malicious activity. Building on this idea, participants discussed how digital twins can serve as a foundation for such behavior-specification-based intrusion detection systems (IDSs) that possess physics- and process-aware capabilities. Moreover, discussions touched on how digital twins can be used for data generation purposes to improve the training phase of (semi-)supervised learning approaches that are employed in behavior-based IDSs.

Attack Response Mechanisms. The last theme was associated with research questions on implementing proactive and reactive attack response strategies, which may represent another use case of digital twins. Proactive security measures can prevent cyber-physical attacks in the face of imminent threats when new vulnerabilities in the CPS are discovered. On the other hand, reactive responses to an attack can be initiated to control damage by ensuring that the physical system maintains a safe state. In this context, questions were raised about how the digital-twin concept can help in designing attack-resilient CPS architectures and response strategies for control systems. This theme highlighted the benefits and challenges of using digital twins to test countermeasures in a simulated environment and assess their effects.

The program started with a welcome session that provided an opportunity for participants to get to know one another. Furthermore, the organizers used this session to share information about the seminar program and explain key terms to participants who were not au fait with the terminologies used by different communities. Over the five days, 14 participants gave lightning talks that focused on the following topics:

- building blocks for digital-twin construction, including emulating and simulating CPS components, data-driven approaches and semantic technologies, synchronization mechanisms,
- reverse engineering programmable logic controllers, deception technology (e.g., honeypots), security testbeds,
- attack detection in CPSs, featuring physics-based, data-driven, and process-aware techniques,
- attack-resilient control using different tools for risk mitigation (viz., prevention, detection, and treatment),
- various aspects of dataset availability in CPS research (e.g., attack simulation, data collection, evaluation, and validation), and
- digital-twin use cases for the safety-related system development lifecycle.

The lightning talk sessions offered each speaker 15 minutes to present new perspectives and talk about current challenges in CPS security. The highly interdisciplinary setting and stimulating presentations given by participants resulted in active discussions, which were carried on in the breakout sessions.

The afternoons of Monday, Tuesday, and Wednesday were used for breakout sessions to give participants the opportunity to work together on research issues of common interest. Based on the discussions that took place on Monday after the session on bridging the disciplinary gap, we identified the following topics of interest to be explored by working groups: (i) conceptualization of the digital twin for cyber-physical systems security, and (ii) attack recovery for control systems. Participants who worked on the former topic discussed

characteristics that digital twins need to have to be useful for security applications, while those who focused on the latter topic investigated strategies in the context of control theory to respond to attacks in a reactive manner.

The seminar received very positive feedback from participants, who also expressed strong interest in future editions. In addition, several invitees, who were forced to cancel their participation at short notice due to the SARS-CoV-2 pandemic, have shown great interest in follow-up events. Thus, we believe that this Dagstuhl Seminar should be repeated in the future. A second edition would be worthwhile to investigate open problems concerning system emulation. These issues could be addressed in a future follow-up seminar if more participation from the embedded systems and systems security communities is achieved.

As the organizers, we would like to thank everyone who attended this seminar for their interesting talks, the thought-provoking questions, and the fruitful contributions that led to a highly collaborative atmosphere for scientific discussions. We also would like to express our sincere gratitude to the scientific and administrative staff of Schloss Dagstuhl for their outstanding support that made this seminar possible.

References

- 1 Henning Kagermann, Johannes Helbig, Ariane Hellinger, and Wolfgang Wahlster. Recommendations for implementing the strategic initiative INDUSTRIE 4.0 – securing the future of german manufacturing industry. Final report of the Industrie 4.0 working group, acatech – National Academy of Science and Engineering, München, April 2013.
- 2 Benjamin Green, Anhtuan Lee, Rob Antrobus, Utz Roedig, David Hutchison, and Awais Rashid. Pains, gains and PLCs: Ten lessons from building an industrial control systems testbed for security research. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*, Vancouver, BC, 2017. USENIX Association.
- 3 David Duggan, Michael Berg, John Dillinger, and Jason Stamp. Penetration testing of industrial control systems. *Sandia National Laboratories*, 2005.
- 4 Mike Shafto, Mike Conroy, Rich Doyle, Ed Glaessgen, Chris Kemp, Jacqueline LeMoigne, and Lui Wang. Draft modeling, simulation, information technology & processing roadmap. *Technology Area*, 11, 2010.
- 5 Elisa Negri, Luca Fumagalli, and Marco Macchi. A review of the roles of digital twin in CPS-based production systems. *Procedia Manufacturing*, 11:939 – 948, 2017. 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy.
- 6 Roland Rosen, Georg von Wichert, George Lo, and Kurt D. Bettenhausen. About the importance of autonomy and digital twins for the future of manufacturing. *IFAC-PapersOnLine*, 48(3):567 – 572, 2015. 15th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2015.
- 7 Werner Kritzing, Matthias Karner, Georg Traar, Jan Henjes, and Wilfried Sihm. Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine*, 51(11):1016 – 1022, 2018. 16th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2018.
- 8 Matthias Eckhart and Andreas Ekelhart. *Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook*, chapter 14, pages 383–412. Springer International Publishing, Cham, 2019.
- 9 Mariana Segovia and Joaquin Garcia-Alfaro. Design, modeling and implementation of digital twins. *Sensors*, 22(14), 2022.
- 10 Marietheres Dietz and Gunther Pernul. Unleashing the digital twin’s potential for ICS security. *IEEE Security & Privacy*, 18(4):20–27, July 2020.

- 11 David Holmes, Maria Papathanasaki, Leandros Maglaras, Mohamed Amine Ferrag, Surya Nepal, and Helge Janicke. Digital twins and cyber security – solution or challenge? In *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, pages 1–8, September 2021.
- 12 Rajiv Faleiro, Lei Pan, Shiva Raj Pokhrel, and Robin Doss. Digital twin for cybersecurity: Towards enhancing cyber resilience. In Wei Xiang, Fengling Han, and Tran Khoa Phan, editors, *Broadband Communications, Networks, and Systems*, pages 57–76, Cham, 2022. Springer International Publishing.
- 13 Abhishek Pokhrel, Vikash Katta, and Ricardo Colomo-Palacios. Digital twin for cybersecurity incident prediction: A multivocal literature review. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pages 671–678, New York, NY, USA, 2020. Association for Computing Machinery.
- 14 Cristina Alcaraz and Javier Lopez. Digital twin: A comprehensive survey of security threats. *IEEE Communications Surveys & Tutorials*, 2022.

2 Table of Contents

Executive Summary

Matthias Eckhart, Alvaro Cárdenas Mora, Simin Nadjm-Tehrani, Edgar Weippl . . . 54

Overview of Talks

Dataset availability and requirements for CPS security research

Magnus Almgren 60

Modelling in the Safety Lifecycle of Radiation Monitoring Systems at CERN

Katharina Ceesay-Seitz 60

Digital Twins for CPS Security

Alvaro Cárdenas Mora 62

A Roadmap Toward a Digital-Twin Framework for Cyber-Physical Systems Security:
Vision, Recent Progress, and Open Challenges

Matthias Eckhart 62

Towards Semantically Enhanced Digital Twins

Helge Janicke 63

Detection of Cyber-Physical Attacks with IIoT data

Marina Krotofil 63

Control-theoretical Analysis of Systems under CPU Starvation Attacks

Martina Maggio 64

RICSel21: Data Collection from Attacks in a Virtual Power Grid

Simin Nadjm-Tehrani 64

Building High Fidelity Replicas for Cyber-Physical Systems Security Research –
Lessons from a Testbeds Programme

Awais Rashid 65

Integrated distributed SCADA security in power grids

Anne Remke 65

Attack-resilient control using model- and data-based intrusion detection

Henrik Sandberg 66

Through the Looking Glass, and What We Found There

Nils Ole Tippenhauer 67

Working Groups

Conceptualization of the Digital Twin for Cyber-Physical Systems Security

Matthias Eckhart 68

Attack Recovery for Control Systems

Martina Maggio 68

Participants 71

3 Overview of Talks

3.1 Dataset availability and requirements for CPS security research

Magnus Almgren (Chalmers University of Technology – Göteborg, SE)

License © Creative Commons BY 4.0 International license
© Magnus Almgren

Joint work of Magnus Almgren, Wissam Aoudi, Mikel Iturbe

Main reference Wissam Aoudi, Mikel Iturbe, Magnus Almgren: “Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems”, in Proc. of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, pp. 817–831, ACM, 2018.

URL <https://doi.org/10.1145/3243734.3243781>

One of the challenges of CPS security research is validating the results, be it through a dataset or by using a real(-alistic) system. The first challenge is to find or create a system or dataset containing the indicators that are used in the algorithm. The second challenge is then to demonstrate different properties: true positives, false positives, true negative, false negatives. The third challenge is then to argue that the attacks or the system under study are realistic, preferably created by someone outside of the research group. One might also need to be able to show a certain set of robustness of the system. All of the above are challenges when it comes to any sort of validation, but more so when it concerns CPS of a societal value.

In the talk, I will outline these challenges by using as a case study the process we used for validating the system presented at CCS 2018.

3.2 Modelling in the Safety Lifecycle of Radiation Monitoring Systems at CERN

Katharina Ceesay-Seitz (CERN – Meyrin, CH)

License © Creative Commons BY 4.0 International license
© Katharina Ceesay-Seitz

Joint work of Katharina Ceesay-Seitz, Hamza Boukabache, Daniel Perrin, Gael Ducos, Sarath Kundumattathil-Mohanalan, Amitabh Yadav

CERN, the European Organisation for Nuclear Research, operates the world’s largest particle accelerator and many other high energy physics experiments. These experiments produce ionizing radiation, for example when particles hit stable matter. The radiation protection group is responsible for protecting humans from any unjustified radiation exposure. The CERN RadiatiOn Monitoring Electronics (CROME) are the new generation of instruments built for measuring ionizing radiation levels and triggering alarms and machine interlocks based on these measurements [1].

Models of subsystems are used throughout the safety lifecycle of CROME. Physics simulations were used to model the expected radiation levels in different zones. Based on these simulations and on the envisioned use cases the system’s functional and safety requirements were defined. Models of subsystems were used throughout the design phase for interoperability and testing purposes.

The CROME Measuring and Processing Unit consists of a radiation detector and an electronic system for data communication and storage, signal processing and safety-related decision taking. It houses a Zynq-7000 System-on-Chip (SoC) consisting of a dual-core ARM processor and an FPGA section. The ARM cores execute an embedded Linux and an

application that receives around 150 parameters via a custom TCP/IP based communication library [2] form a SCADA system [3]. An independent test tool has been developed to model the library's functionalities [4]. It has been used to strengthen the robustness of the design by sending malformed messages to CROME and observing its response.

The parameters, which can be floating point variables or integers with ranges up to 64 bit, or others, are processed and sent to the FPGA, which performs all safety critical calculations and decision making. It calculates the radiation dose received in a given time as well as the dose rate from the input received from the radiation detector. Based on these measurements and the current parameter configuration, it can autonomously trigger alarms and machine interlocks. Models with different levels of abstraction are used to verify the functionality of the system. Constrained-random simulation has been used to simulate a large state space, which led to the discovery of several faults. Simulation only covers a subset of the possible states. Many additional faults have been found with formal verification, even in scenarios that were impossible to simulate due to the real-time nature of the system [5]. Formal verification has also been successfully used for the partial verification of a prototype of the future frontend of CROME, the ACCURATE 2 ASIC for ultra-low current measurement [7, 6].


This talk presents the different modelling approaches and discusses potential use cases for digital twins.

References

- 1 Hamza Boukabache, Michel Pangallo, Gael Ducos, Nicola Cardines, Antonio Bellotta, Ciarán Toner, Daniel Perrin, and Doris Forkel-Wirth. Towards a novel modular architecture for CERN radiation monitoring. *Radiation Protection Dosimetry*, 173(1-3):240–244, November 2016.
- 2 Amitabh Yadav, Hamza Boukabache, Katharina Ceesay-Seitz, Nicola Gerber, and Daniel Perrin. ROMULUSLib: An autonomous, TCP/IP-based, multi-architecture C networking library for DAQ and control applications. *Proceedings of the 18th International Conference on Accelerator and Large Experimental Physics Control Systems*, ICALEPCS2021:69–76, 2022.
- 3 Adrien Ledeul, Alexandru Savulescu, Gustavo Segura, Bartłomiej Styczen, and Daniel Vazquez Rivera. CERN supervision, control and data acquisition system for radiation and environmental protection. *Proceedings of the 12th Int. Workshop on Emerging Technologies and Scientific Facilities Controls*, PCaPAC2018:248–252, 2019.
- 4 Katharina Ceesay-Seitz, Hamza Boukabache, Marvin Leveneur, and Daniel Perrin. RomLibEmu: Network interface stress tests for the CERN radiation monitoring electronics (CROME). *Proceedings of the 18th International Conference on Accelerator and Large Experimental Physics Control Systems*, ICALEPCS2021:581–585, 2022.
- 5 Katharina Ceesay-Seitz, Hamza Boukabache, and Daniel Perrin. A functional verification methodology for highly parametrizable, continuously operating safety-critical FPGA designs: Applied to the CERN RadiatiOn monitoring electronics (CROME). In António Casimiro, Frank Ortmeier, Friedemann Bitsch, and Pedro Ferreira, editors, *Computer Safety, Reliability, and Security*, pages 67–81, Cham, 2020. Springer International Publishing.
- 6 Katharina Ceesay-Seitz, Sarath Kundumattathil Mohanan, Hamza Boukabache, Daniel Perrin, and Hamza Boukabache. Formal property verification of the digital section of an ultra-low current digitizer ASIC. In *Design and Verification Conference in Europe*, October 2021.
- 7 Sarath Kundumattathil Mohanan, Hamza Boukabache, Vassili Cruchet, Daniel Perrin, Stefan Roesler, and Ullrich R. Pfeiffer. An ultra low current measurement mixed-signal ASIC for radiation monitoring using ionisation chambers. *IEEE Sensors Journal*, 22(3):2142–2150, February 2022.

3.3 Digital Twins for CPS Security

Alvaro Cárdenas Mora (University of California – Santa Cruz, US)

License  Creative Commons BY 4.0 International license
© Alvaro Cárdenas Mora


In this talk we discuss the differences between IT and OT security, and how digital twins for physical systems are a natural component to address the new challenges of OT security.

Then we discuss our work on how digital twins can help in security by:

- Deploy new defenses such as attack recovery
- Understand the consequences of attacks and risks of CPS
- Interact with the adversary (Through honeypots or by executing malware in a contained setting)
- Finding new attacks in a principled manner (e.g., fuzzing the physical system).

3.4 A Roadmap Toward a Digital-Twin Framework for Cyber-Physical Systems Security: Vision, Recent Progress, and Open Challenges

Matthias Eckhart (SBA Research – Wien, AT)

License  Creative Commons BY 4.0 International license
© Matthias Eckhart

Joint work of Matthias Eckhart, Andreas Ekelhart

The term “digital twin” is one of the latest technology buzzwords that has emerged along with the digital transformation that is taking place in CPS domains. Since there is no generally accepted definition of this term yet, the understanding of the digital-twin concept is often limited to the notion that a cyber-physical system is replicated in a digitally-enhanced way. This talk provides one interpretation of digital twins by breaking down the concept into four components that are required to implement them, viz., i) system emulation or via system containers, including I/O simulation, ii) network emulation, iii) interactive, real-time simulation of the physical process, and iv) synchronization with the physical counterparts. After putting the digital-twin concept into context, we present our current progress on developing a framework named CPS Twinning that integrates these four components for the purpose of generating such digital twins, so that security applications (e.g., intrusion detection) can be built on top. The talk concludes with an overview of open challenges and research opportunities in this area.

References

- 1 Matthias Eckhart and Andreas Ekelhart. *Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook*, chapter 14, pages 383–412. Springer International Publishing, Cham, 2019.
- 2 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*, CPS-SPC '18, pages 36–47, New York, NY, USA, 2018. ACM.
- 3 Matthias Eckhart, Andreas Ekelhart, and Roland Eisl. Digital twins for cyber-physical threat detection and response. *ERCIM News*, 2021(127), 2021.
- 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 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, CPSS '18*, pages 61–72, New York, NY, USA, 2018. ACM.
- 6 Matthias Eckhart and Andreas Ekelhart. Securing cyber-physical systems through digital twins. *ERCIM News*, 2018(115), 2018.

3.5 Towards Semantically Enhanced Digital Twins

Helge Janicke (Cyber Security CRS – Joondalup, AU)

License © Creative Commons BY 4.0 International license
© Helge Janicke

Joint work of Helge Janicke, David Holmes, Surya Nepal

Main reference David Holmes, Maria Papathanasaki, Leandros A. Maglaras, Mohamed Amine Ferrag, Surya Nepal, Helge Janicke: “Digital Twins and Cyber Security – solution or challenge?”, in Proc. of the 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference, SEEDA-CECNSM 2021, Preveza, Greece, September 24-26, 2021, pp. 1–8, IEEE, 2021.

URL <https://doi.org/10.1109/SEEDA-CECNSM53056.2021.9566277>

Digital twin technology today is diverse and emerging and its full potential is not yet widely understood. The concept of a digital twin allows for the analysis, design, optimisation and evolution of systems to take place fully digital, or in conjunction with a cyber-physical system to improve speed, accuracy and efficiency when compared to traditional engineering approaches. Digital Twin technology is mainly used today as a digital replica of a physical system with the generated and observed data being used for applications such as predictive maintenance, fault analysis and optimisation. This is predominantly a data-driven approach that uses modern machine learning technologies to maximise the benefit of the available data. This talk proposes the semantic markup of digital twins to unlock the benefits of other aspects of Artificial Intelligence, namely semantic reasoning, to broaden the application facilitate deeper analysis of systems and their properties than can be achieved by analysing their data and behaviours through observation. The talk will explore potential synergies and barriers that need to be overcome for this approach to unlock future digital twin applications.

3.6 Detection of Cyber-Physical Attacks with IIoT data

Marina Krotofil (Maersk – Aarhus, DK)

License © Creative Commons BY 4.0 International license
© Marina Krotofil

Novel IIoT architectures such as NOA (NAMUR Open Architecture) allow for delivery of raw or high-resolution IIoT data via dedicated data highways. This data is used for various purposes such as developing digital twin models, predictive maintenance and augmented reality applications, etc. These data can also be used as a source of forensic artefacts or even evidence when investigating cyber-physical attacks. In this talk we will show a specific example of how IIoT data is used to detect an ongoing attack on an industrial pump and determine its root cause. We will leave the audience with an open question about the requirement to the collection, transport and storage of IoT data to ensure their utility to incident response and admissibility as legal evidence.

3.7 Control-theoretical Analysis of Systems under CPU Starvation Attacks

Martina Maggio (Universität des Saarlandes – Saarbrücken, DE)

License © Creative Commons BY 4.0 International license

© Martina Maggio

Joint work of Martina Maggio, Martin Gunnarsson, Nils Vreman

Embedded systems and cyber-physical controllers have been proven vulnerable to security attacks of various nature, including man-in-the-middle attacks that alter sensor data and actuator commands, and attacks that disrupt the calculation of the control signals. While attack detection has been widely studied, countermeasures are scarce at best. We propose and implement a defence technique, based on executing the controller code in a trusted execution environment.

3.8 RICSel21: Data Collection from Attacks in a Virtual Power Grid

Simin Nadjm-Tehrani (Linköping University, SE)

License © Creative Commons BY 4.0 International license

© Simin Nadjm-Tehrani

Joint work of Simin Nadjm-Tehrani, Chih-Yuan Lin, August Fundin, Eric Westring, Tommy Gustavsson

Main reference Chih-Yuan Lin, August Fundin, Erik Westring, Tommy Gustafsson, Simin Nadim-Tehrani: “RICSel21 Data Collection: Attacks in a Virtual Power Network”, in Proc. of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2021, Aachen, Germany, October 25-28, 2021, pp. 201–206, IEEE, 2021.

URL <https://doi.org/10.1109/SmartGridComm51999.2021.9632328>

In this talk I give an overview of the work done in one of the three tracks within the Swedish research centre on Resilient Information and Control Systems (RICS) [2]. The three tracks involve a) Data emulation b) Attack modelling and risk analysis, and c) Anomaly detection. The work on the Data emulation part has resulted in a national virtual testbed RICS-el for Supervisory Control and Data Acquisition (SCADA) security analysis in an electricity distribution network with a commercial SCADA software, some 20 emulated substations connected with wide area networks, OT, DMZ and IT segments. It has so far been exposed in two published works in collaboration with several colleagues [3, 1]. This talk focuses on the latest publication where 12 attacks were performed in the testbed and the outcomes documented. The dataset from the attack scenarios and the baseline (no-attack) counterpart is available for sharing.

References

- 1 Chih-Yuan Lin, August Fundin, Erik Westring, Tommy Gustafsson, and Simin Nadim-Tehrani. RICSel21: Data collection: Attacks in a virtual power network. In *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 201–206, October 2021.
- 2 Simin Nadjm-Tehrani, Mathias Ekstedt, and Magnus Almgren. RICS: Research centre on resilient information and control systems, 2022. Available: <https://www.rics.se/>
- 3 Magnus Almgren, Peter Andersson, Gunnar Björkman, Mathias Ekstedt, Jonas Hallberg, Simin Nadjm-Tehrani, and Erik Westring. RICS-el: Building a national testbed for research and training on SCADA security (short paper). In Eric Luijff, Inga Žutautaitė, and Bernhard M. Hämmerli, editors, *Critical Information Infrastructures Security*, pages 219–225, Cham, 2019. Springer International Publishing.

3.9 Building High Fidelity Replicas for Cyber-Physical Systems Security Research – Lessons from a Testbeds Programme

Awais Rashid (University of Bristol, GB)

License © Creative Commons BY 4.0 International license

© Awais Rashid

Joint work of Awais Rashid, Rob Antrobus, Barnaby Craggs, Joseph Gardiner, Benjamin Green, David Hutchison, Anhtuan Lee, Utz Roedig

Main reference Joseph Gardiner, Barnaby Craggs, Benjamin Green, Awais Rashid: “Oops I Did it Again: Further Adventures in the Land of ICS Security Testbeds”, in Proc. of the ACM Workshop on Cyber-Physical Systems Security & Privacy, CPS-SPC@CCS 2019, London, UK, November 11, 2019, pp. 75–86, ACM, 2019.

URL <https://doi.org/10.1145/3338499.3357355>

Digital twins aim to provide an extensive and scalable means to model and evaluate properties of real-world systems. Developing such digital twins for cyber-physical systems is non-trivial even more so at a high enough fidelity in order to suitably replicate behaviours of real-world systems when compromised or under attack. In this talk, I will reflect on experiences of over 8 years of research building cyber-physical systems security testbeds particularly those to support security analyses of industrial control systems. I will discuss challenges arising from the need to represent a diversity of devices, networking mechanisms and software platforms as well as scalability of experimentation and managing the complexity of the testbed environment itself. I will reflect on what research on digital twins can learn from these experiences and the potential for “physical” testbed environments to work in tandem with digital twins.

References

- 1 Joseph Gardiner, Barnaby Craggs, Benjamin Green, and Awais Rashid. Oops i did it again: Further adventures in the land of ICS security testbeds. In *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy, CPS-SPC'19*, pages 75–86, New York, NY, USA, 2019. Association for Computing Machinery.
- 2 Benjamin Green, Anhtuan Lee, Rob Antrobus, Utz Roedig, David Hutchison, and Awais Rashid. Pains, gains and PLCs: Ten lessons from building an industrial control systems testbed for security research. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*, Vancouver, BC, 2017. USENIX Association.
- 3 Awais Rashid, Joseph Gardiner, Benjamin Green, and Barnaby Craggs. Everything is awesome! or is it? cyber security risks in critical infrastructure. In Simin Nadjm-Tehrani, editor, *Critical Information Infrastructures Security*, pages 3–17, Cham, 2020. Springer International Publishing.

3.10 Integrated distributed SCADA security in power grids

Anne Remke (Universität Münster, DE)

License © Creative Commons BY 4.0 International license

© Anne Remke

Joint work of Anne Remke, Verena Menzel, Johann Hurink

Main reference Verena Menzel, Johann L. Hurink, Anne Remke: “Securing SCADA networks for smart grids via a distributed evaluation of local sensor data”, in Proc. of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2021, Aachen, Germany, October 25–28, 2021, pp. 405–411, IEEE, 2021.

URL <https://doi.org/10.1109/SmartGridComm51999.2021.9632283>

Within smart grids the safe and dependable distribution of electric power highly depends on the security of Supervisory Control and Data Acquisition (SCADA) systems and their underlying communication protocols. Existing network-based intrusion detection systems for

Industrial Control Systems (ICS) are usually centrally applied at the SCADA server and do not take the underlying physical process into account. A recent line of work proposes an additional layer of security via a process-aware approach applied locally at the field stations. Currently, we broaden the scope of process-aware monitoring by considering the interaction between neighboring field stations, which facilitates upcoming trends of decentralized energy management (DEM). Local security monitoring is lifted to monitoring neighborhoods of field stations, therefore achieving a broader grid coverage w.r.t. security. We provide a distributed monitoring algorithm of the generated sensory readings for this extended setting. The feasibility of the approach is shown via a prototype simulation testbed and a scenario with two subgrids.

3.11 Attack-resilient control using model- and data-based intrusion detection

Henrik Sandberg (KTH Royal Institute of Technology – Stockholm, SE)

License © Creative Commons BY 4.0 International license
© Henrik Sandberg

Joint work of Henrik Sandberg, Kaveh Paridari, Niamh O'Mahony, Alie El-Din Mady, Rohan Chabukswar, Menouer Boubekeur, David Umsonst

Main reference Kaveh Paridari, Niamh O'Mahony, Alie El-Din Mady, Rohan Chabukswar, Menouer Boubekeur, Henrik Sandberg: "A Framework for Attack-Resilient Industrial Control Systems: Attack Detection and Controller Reconfiguration", *Proc. IEEE*, Vol. 106(1), pp. 113–128, 2018.

URL <https://doi.org/10.1109/JPROC.2017.2725482>

Main reference David Umsonst, Henrik Sandberg: "On the confidentiality of controller states under sensor attacks", *Autom.*, Vol. 123, p. 109329, 2021.

URL <https://doi.org/10.1016/j.automatica.2020.109329>

In this talk, we discuss two aspects of model- and data-based intrusion detection. First, we show how a centralized model- and data-based intrusion detector in an industrial control system can use analytical redundancy to first detect and then reconstruct attacked signals in local feedback loops, to achieve resilience. We discuss pros and cons of the model- and data-based detection schemes. Second, we discuss a necessary and sufficient condition for an adversary with access to sensor data to replicate the state of the control system, and in extension the intrusion detection system. Advanced adversaries use such state information to launch stealthy attacks, and our condition gives insights as to how to block such attacks. The condition also provides insights on the possibilities for adversaries to replicate and synchronize with the state of digital twins.

The talk is based on the following papers: [1, 2].

References

- 1 Kaveh Paridari, Niamh O'Mahony, Alie El-Din Mady, Rohan Chabukswar, Menouer Boubekeur, and Henrik Sandberg. A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration. *Proceedings of the IEEE*, 106(1):113–128, January 2018.
- 2 David Umsonst and Henrik Sandberg. On the confidentiality of controller states under sensor attacks. *Automatica*, 123:109329, 2021.

3.12 Through the Looking Glass, and What We Found There

Nils Ole Tippenhauer (CISPA – Saarbrücken, DE)

License © Creative Commons BY 4.0 International license
© Nils Ole Tippenhauer

Main reference Daniele Antonioli, Nils Ole Tippenhauer: “MiniCPS: A Toolkit for Security Research on CPS Networks”, in Proc. of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC 2015, Denver, Colorado, USA, October 16, 2015, pp. 91–100, ACM, 2015.

URL <https://doi.org/10.1145/2808705.2808715>

In this talk, we reflect on our research journey in the area of cybersecurity for industrial control systems. During our work on GPS spoofing [1], we noted two main challenges for precise GPS spoofing: i) the attacker needs to accurately create spoofed GPS signals (i.e., their signal strength, timing, etc), and ii) the attacker needs to carefully start the attack to slowly divert the victim’s state estimation (assuming prior synchronization to legitimate GPS signals) from the legitimate to the manipulated state. Such challenges that introduce control theoretic approaches to cybersecurity motivated us to further investigate cybersecurity for general Cyber-Physical Systems, in particular industrial control systems. To understand and experiment with such systems, we built several testbeds at SUTD in Singapore [2], and designed the MiniCPS framework [3] to emulate those environments. The resulting datasets turned out to be very useful for training and evaluation of process-aware attack detection systems [4, 5]. We also realized that tools such as MiniCPS could enable the construction of to *digital twins* – for example to be used as Honeynets, reference in anomaly detection, and for attack development and verification.

References

- 1 Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS ’11*, pages 75–86, New York, NY, USA, 2011. Association for Computing Machinery.
- 2 A. P. Mathur and N. O. Tippenhauer. SWaT: A water treatment testbed for research and training on ICS security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, pages 31–36, April 2016.
- 3 Daniele Antonioli and Nils Ole Tippenhauer. MiniCPS: A toolkit for security research on CPS networks. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC ’15*, pages 91–100, New York, NY, USA, 2015. ACM.
- 4 Riccardo Taormina, Stefano Galelli, Nils Ole Tippenhauer, Elad Salomons, Avi Ostfeld, Demetrios G. Eliades, Mohsen Aghashahi, Raanju Sundararajan, Mohsen Pourahmadi, M. Katherine Banks, B. M. Brentan, Enrique Campbell, G. Lima, D. Manzi, D. Ayala-Cabrera, M. Herrera, I. Montalvo, J. Izquierdo, E. Luvizotto, Sarin E. Chandy, Amin Rasekh, Zachary A. Barker, Bruce Campbell, M. Ehsan Shafiee, Marcio Giacomoni, Nikolaos Gatsis, Ahmad Taha, Ahmed A. Abokifa, Kelsey Haddad, Cynthia S. Lo, Pratim Biswas, M. Fayzul K. Pasha, Bijay Kc, Saravanakumar Lakshmanan Somasundaram, Mashor Housh, and Ziv Ohar. Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks. *Journal of Water Resources Planning and Management*, 144(8):04018048, 2018.
- 5 Alessandro Erba, Riccardo Taormina, Stefano Galelli, Marcello Pogliani, Michele Carminati, Stefano Zanero, and Nils Ole Tippenhauer. Constrained concealment attacks against reconstruction-based anomaly detectors in industrial control systems. In *Annual Computer Security Applications Conference, ACSAC ’20*, pages 480–495, New York, NY, USA, 2020. Association for Computing Machinery.

4 Working Groups

4.1 Conceptualization of the Digital Twin for Cyber-Physical Systems Security

Matthias Eckhart (SBA Research – Wien, AT)

License © Creative Commons BY 4.0 International license

© Matthias Eckhart

Joint work of Matthias Eckhart, David Allison, Magnus Almgren, Katharina Ceesay-Seitz, Andreas Ekelhart, Helge Janicke, Simin Nadjm-Tehrani, Awais Rashid, Edgar Weippl, Mark Yampolskiy

The objective of this working group was to (i) analyze the potential characteristics of digital twins, (ii) identify security-relevant purposes, and (iii) create a mapping between the two to inform security researchers and practitioners about the characteristics that are required to implement a certain purpose. The first breakout session kicked off with a brainstorming exercise to decompose the research problem at hand into a set of questions, namely:

- In the context of the barest definition of the term, what would qualify as a digital twin?
- How does a digital twin differ from a digital representation of a physical entity that may be implemented as a data-driven model, 3D visual model, or simulation?
- How can the fidelity of a digital twin be defined and measured?
- On which CPS layers should digital twins function?
- What does synchronization in the context of digital twins mean?
- To what extent is synchronization between the digital twin and its counterpart necessary?
- How can a synchronization mechanism be implemented that covers the physics, application, network, and user layers?
- For which cases would a bidirectional connection between the CPS and the digital twin(s) be necessary?
- How would the time and methodology of digital-twin construction differ for certain activities within the CPS lifecycle?
- What is the value of a digital twin in terms of improving the security of CPSs?
- How do digital twins differ from honeypots and cyber ranges (i.e., security testbeds)?

The rationale behind asking these questions was to explore and identify different characteristics that define security-focused digital twins. During the breakout sessions, the participants engaged in vivid discussions that generated an initial draft of definitions. The group then assigned those characteristics to security-relevant purposes, indicating which features a digital twin should possess to be useful for addressing well-known cybersecurity challenges. A summary of the results is currently in preparation and will be submitted for peer review in the upcoming months.

4.2 Attack Recovery for Control Systems

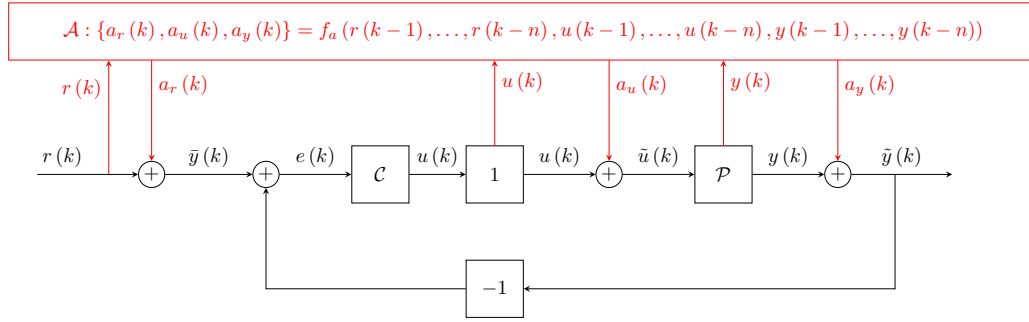
Martina Maggio (Universität des Saarlandes – Saarbrücken, DE)

License © Creative Commons BY 4.0 International license

© Martina Maggio

Joint work of Martina Maggio, Ali Abbasi, Alvaro Cárdenas Mora, Marina Krotofil, Miroslav Pajic, Awais Rashid, Francesco Regazzoni, Anne Remke, Henrik Sandberg, Anne-Kathrin Schmuck, Nils Ole Tippenhauer

In this working group, we discussed *digital-twin approved recovery* strategies. Suppose that an attack is ongoing and has been detected, the discussion centred around “what kind of manoeuvres are safe after an attack has been identified”?



■ **Figure 1** General attack model.

Generally speaking, we identified different goals for attack recovery:

- Recovery
- Resilience (long-term recovery)
- Safe shutdown or graceful degradation
- Survivability (we could test on the digital twin that the system would survive a catastrophic event)
- Mission completion

In this context, we moved onto discussing the actual possible actions that can be taken as a response to the attack and a potential modelling of the attack.

In Figure 1, we identify how a control system and its digital twin would look like. The variable k counts time iterations. A setpoint $r(k)$ is provided to the system (a drone should reach a given point in a tri-dimensional space). This setpoint can be intercepted and attacked using a signal $a_r(k)$ that is summed to the actual given setpoint (this models any replacement of the setpoint value). The controller then receives $\bar{y}(k)$ and calculates an error signal $e(k)$ that determines the current distance from the setpoint. This value is used by the controller to calculate a control signal $u(k)$, that is then sent to a plant. An attacker can intercept the sensor data and modify the control signal. This is modelled using a value $a_u(k)$ that is calculated by the attacker and summed to the received control signal, forming $\tilde{u}(k)$, which is fed to the plant. The plant then executes and physical values $y(k)$ are sensed. Sensors can also be attacked, via a signal $a_y(k)$, generated by the attacker.

The blocks \mathcal{C} , 1 , and -1 can be augmented with knowledge from the plant (for example: typical execution delays, typical network delays, typical probability of not receiving packets over the network, etc). The block \mathcal{P} can be augmented with knowledge from the physics (for example: acceptable values for friction and stiction coefficients). This knowledge augments the blocks forming the *digital twin*, and can be exploited by the recovery mechanism to detect and react to unusual situations. For example, if the controller execution time is longer than expected, the digital twin can suspect an attack.

A consideration that emerged is that while normally the controller closes the loop around a physical system, during the recovery period the system runs in open loop and can and must not trust the input data it receives from the sensors, because they would be compromised. In this situation, the detection of the attack could lead us to understand and estimate when the attack started and hence when the last reliable data was received by the controller. The digital twin could then be used to fast forward the execution of the controller and estimate the state of the actual system that received control signals that were calculated based on

compromised data. The digital twin could also be used to understand what are good control signal to apply while the system is running in open loop. From the control perspective, this can for example be done running a model predictive control algorithm.

Participants

- Ali Abbasi
Ruhr-Universität Bochum, DE
- David Allison
AIT – Austrian Institute of
Technology – Wien, AT
- Magnus Almgren
Chalmers University of
Technology – Göteborg, SE
- Alvaro Cárdenas Mora
University of California –
Santa Cruz, US
- Katharina Ceesay-Seitz
CERN – Meyrin, CH
- Matthias Eckhart
SBA Research – Wien, AT
- Andreas Ekelhart
SBA Research – Wien, AT
- Helge Janicke
Cyber Security CRS –
Joondalup, AU
- Marina Krotofil
Maersk – Aarhus, DK
- Martina Maggio
Universität des Saarlandes –
Saarbrücken, DE
- Simin Nadjm-Tehrani
Linköping University, SE
- Miroslav Pajic
Duke University – Durham, US
- Awais Rashid
University of Bristol, GB
- Francesco Regazzoni
University of Amsterdam, NL &
Università della Svizzera
italiana, CH
- Anne Remke
Universität Münster, DE
- Henrik Sandberg
KTH Royal Institute of
Technology – Stockholm, SE
- Anne-Kathrin Schmuck
MPI-SWS – Kaiserslautern, DE
- Nils Ole Tippenhauer
CISPA – Saarbrücken, DE
- Edgar Weippl
University of Vienna & SBA
Research – Wien, AT
- Mark Yampolskiy
Auburn University, US

