Thesis for The Degree of Doctor of Philosophy

Process-Aware Defenses for Cyber-Physical Systems

Wissam Aoudi

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden, 2021

Process-Aware Defenses for Cyber-Physical Systems

Wissam Aoudi

ISBN 978-91-7905-503-5
Doktorsavhandlingar vid Chalmers tekniska högskola, Ny serie nr 4970.
ISSN 0346-718X

Technical Report No 199D
Department of Computer Science & Engineering
Chalmers University of Technology
SE-412 96 Gothenburg, Sweden
Phone: +46 (0)31-772 10 00

Author e-mail: wissam.aoudi@chalmers.se

This thesis has been prepared using LaTeX.
Printed by Chalmers Reproservice,
Gothenburg, Sweden 2021.

Process-Aware Defenses for Cyber-Physical Systems

Wissam Aoudi
Department of Computer Science & Engineering
Chalmers University of Technology

Abstract

The increasing connectivity is exposing safety-critical systems to cyberattacks that can cause real physical damage and jeopardize human lives. With billions of IoT devices added to the Internet every year, the cybersecurity landscape is drastically shifting from IT systems and networks to systems that comprise both cyber and physical components, commonly referred to as cyber-physical systems (CPS). The difficulty of applying classical IT security solutions in CPS environments has given rise to new security techniques known as process-aware defense mechanisms, which are designed to monitor and protect industrial processes supervised and controlled by cyber elements from sabotage attempts via cyberattacks.

In this thesis, we critically examine the emerging CPS-driven cybersecurity landscape and investigate how process-aware defenses can contribute to the sustainability of highly connected cyber-physical systems by making them less susceptible to crippling cyber-attacks. We introduce a novel data-driven model-free methodology for real-time monitoring of physical processes to detect and report suspicious behaviour before damage occurs. We show how our model-free approach is very lightweight, does not require detailed specifications, and is applicable in various CPS environments including IoT systems and networks. We further design, implement, evaluate, and deploy process-aware techniques, study their efficacy and applicability in real-world settings, and address their deployment challenges.

Keywords: process-aware defenses; cyber-physical systems; industrial control systems; singular spectrum analysis; stealthy attacks

List of Publications

Appended publications

This thesis is based on the work contained in the following publications:

[A] **Wissam Aoudi**, Mikel Iturbe, Magnus Almgren
"Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems"
The 25^{th} ACM Conference on Computer and Communications Security (CCS '18), October 15–19, 2018, Toronto, ON, Canada.

[B] **Wissam Aoudi**, Magnus Almgren
"A Framework for Determining Robust Context-Aware Attack-Detection Thresholds for Cyber-Physical Systems"
The Australasian Information Security Conference (AISC '21), February 01, 2021, Dunedin, New Zealand.

[C] **Wissam Aoudi**, Magnus Almgren
"A Scalable Specification-Agnostic Multi-Sensor Anomaly Detection System for IIoT Environments"
The International Journal of Critical Infrastructure Protection, Volume 30, September 20, 2020.

[D] **Wissam Aoudi**, Nasser Nowdehi, Magnus Almgren, Tomas Olovsson
"Spectra: Detecting Attacks on In-Vehicle Networks through Spectral Analysis of CAN-Message Payloads"
The 36^{th} ACM Symposium on Applied Computing (SAC '21), March 22, 2021, Gwangju, South Korea.

[E] Mohammed Seifu Kemal, **Wissam Aoudi**, Rasmus Olsen, Magnus Almgren, Hans-Peter Schwefel
"Model-Free Detection of Cyberattacks on Voltage Control in Distribution Grids"
The 15^{th} European Dependable Computing Conference (EDCC '19), September 17–20, 2019, Naples, Italy.

[F] Magnus Almgren, **Wissam Aoudi**, Robert Gustafsson, Robin Krahl, Andreas Lindhé
"The Nuts and Bolts of Deploying Process-Level IDS in Industrial Control Systems"
The 4^{th} Annual Workshop on Industrial Control Systems Security (ICSS '18), December 4, 2018, San Juan, Puerto Rico, USA.

[G] **Wissam Aoudi**, Albin Hellqvist, Albert Overland, Magnus Almgren
"A Probe into Process-Level Attack Detection in Industrial Environments from a Side-Channel Perspective"
The 5^{th} Annual Workshop on Industrial Control Systems Security (ICSS '19), December 10, 2019, San Juan, Puerto Rico, USA.

Personal Contribution

In all the appended papers, I led the writing of the manuscripts and collaborated with all other authors. I contributed to **Paper A**, **Paper B**, **Paper C**, and **Paper D** as the lead designer and main implementer.

In **Paper A**, Mikel Iturbe contributed in a major way in designing the attacks and the attacker model, and setting up and running experiments with the Tennessee-Eastman process.

In **Paper D**, Nasser Nowdehi had the leading role in designing and setting up the experiments, defining the attacker model, providing the technical background and the prior art.

In **Paper E**, **Paper F**, and **Paper G**, I contributed to formulating the research problem, designing and implementing algorithms as well as performing extensive experiments.

Acknowledgment

I am grateful to my supervisor Magnus for being such an inspiring mentor. I would have hardly accomplished this thesis without your generous advice and continuous guidance. Thank you for your honesty, diligence, and kindliness!

I would also like to thank MSB for supporting my research, and everyone in the Computer Science and Engineering department at Chalmers, especially the Networks and Systems division, for the stimulating and enriching work environment.

My special thanks go to my beloved wife Malak for the tremendous support throughout my bumpy journey. Thank you for making it all possible!

I extend my gratitude to all other family members and friends for their encouragement, support, and advice.

Contents

Part I

Introduction

1 Thesis Overview

Modern societies are becoming growingly dependent on critical infrastructure operated by industrial control systems (ICS) that are heading towards increased connectivity to scale and meet efficiency requirements [1]. Leveraging advances in information and communication technologies is paving the way for unprecedented efficacy and flexibility of operation. However, through digitalization and inter-connectivity, the Industrial Internet of Things (IIoT) is transforming our critical infrastructure and reshaping the cyber landscape into one with much higher destructive potential [2]. In particular, connectivity and digitalization of control systems open doors to malicious actors with high motivation and resources to remotely compromise these historically isolated systems [3], thereby posing imminent threats to critical infrastructure on which societies highly depend; including health care, transportation, manufacturing, and power distribution to name a few.

Unfortunately, the need for meeting efficiency requirements and enabling more controllability and interfacing with industrial assets is overshadowing the thought of resilient and sustainable modernized infrastructure, and cyber adversaries are becoming ever more capable in the process. Unlike attacks on IT systems that are often bounded by virtual impact, attacks on ICS are of a different nature and can cause physical damage to critical infrastructure [4–10], potentially leading to loss of human lives or large-scale infrastructural chaos. For instance, a cyberattack on a nation's power grid, which could be launched from anywhere in the

world, has been shown capable of depriving thousands of households and facilities of electricity [11].

The need to secure control systems is unquestionable and efforts to secure them are increasing, albeit at a relatively modest pace in light of the scale and nature of the looming threats. Securing ICS solely from an IT perspective, while necessary, proves insufficient because, at the physical layer, the critical process would remain unmonitored and therefore vulnerable to sabotage by the attackers. At this layer, traditional IT-based security mechanisms are often inapplicable, hence many attempts to detect attacks via direct application of off-the-shelf techniques are doomed to fall short.

One approach that has proven viable in recent years proposes to monitor the *process-level* network connecting field devices to detect intrusions [12–18]. This thesis, at its core, is a continuation of this line of research work as it contributes a novel model-free approach with key favourable features to detecting cyberattacks on ICS by monitoring the process network in real time and deciding when the system operation is departing from normal dynamics.

Besides the introductory part, the thesis consists of three parts addressing both the theoretical and practical aspects of securing cyber-physical systems.

In the first part, we present our novel approach to process-level attack-detection that is rooted in state-of-the-art time-series analysis techniques and adapted to detecting cyberattacks on industrial control systems by monitoring process sensors. We show how using a model-free approach, as opposed to existing model-based approaches, significantly improves the detection accuracy, limits the need for process knowledge, and widens the spectrum of applicable systems. We then identify detection thresholds as a key parameter for process-aware defense techniques and propose a framework for determining thresholds that are suitable for CPS environments.

In the second part, we generalize our approach to cyber-physical systems and industrial IoT environments. We show how, by virtue of the specification-agnostic feature, our proposed technique can be applied to industrial environments employing a multitude of sensors, thereby offering invaluable safety and security insight into the underlying process to operators and stakeholders. We further demonstrate with a proven application that even systems as complex

as modern connected vehicles can be efficiently monitored with model-free process-aware defenses.

In the third part, we investigate the deployment of process-aware defense mechanisms in real industrial environments. We identify deployment challenges and best practices, and report lessons learned from real-world experiments. We also show how using such techniques for side-channel analysis is a viable deployment strategy.

1.1 Background

In the previous section, we defined the research problem and motivated the work in this thesis by highlighting the growing exposure and expanding attack surface of safety-critical systems. In this section, we provide the background on intrusion detection and the security aspects of two representative types of cyber-physical systems, namely control systems and modern vehicles.

1.1.1 Intrusion Detection

Intrusion detection arguably has its academic roots in the 1987 work by Denning [19] and has been extensively studied in the context of typical IT systems ever since. In a broad sense, intrusion detection is divided into two main categories: misuse detection and anomaly detection [20]. In misuse detection, traffic patterns that match with predefined so-called attack signatures are flagged as anomalous while all other traffic is considered normal. By contrast, anomaly detection involves creating a baseline from traffic data defining the normal behavior such that all other traffic that deviates from the baseline is considered anomalous.

In response to the rising cyber threats to critical infrastructure, considerable effort has recently been devoted by the research community to investigating proper defensive measures. Designing intrusion detection systems suitable for cyber-physical environments has been at the forefront of this effort [12–18].

Intrusion detection systems are considered as an important piece of the puzzle because one indispensable step in combating adversarial acts in CPS, or any information system for that matter, is in fact detecting the presence of the attacker. Defining attack signatures in CPS environments is tricky due to the attacks on CPS being rare,

specialized, and targeted at complex system components that are often legacy and proprietary. On the other hand, anomaly-based intrusion detection, although less favorable in IT environments due to intolerably high false-positive rates, proves more adequate for CPS environments due to the regularity in machine-to-machine communication.

1.1.2 Industrial Control Systems (ICS)

Industrial control systems are cyber-physical systems that enable communication between field devices (actuators and sensors) and controllers in a closed-loop fashion to control a physical process. Abstractly considered, closed-loop control systems involve sensors that sense some physical property from the controlled process and communicate the measurements to a controller. Based on the received sensor measurements and on the implemented control logic, controllers send commands to actuators that directly manipulate the physical process to maintain a desired state of operation [1]. The controlled physical process is often sophisticated, cost-sensitive, and high-precision, and ICS are typically found in safety-critical environments. No matter if it is due to failure or malicious acts, undesired changes in the dynamics of these systems may prove highly costly and it is imperative that proper mechanisms are in place to detect them.

The machine-to-machine communication in ICS process networks produces traffic that is highly deterministic, thereby enabling data-driven methods as a viable approach to attack-detection in these environments. Highly regular communication enables reliably constructing a baseline from historical process data and subsequently detecting deviant behavior due to anomalous operation.

1.1.3 Security Aspects of Connected Mobility

Securing the fragile In-Vehicle Networks (IVNs) has recently attracted notable attention as real-world attacks have demonstrated that it is possible to remotely control vehicles and compromise safety-critical functions via, for example, the Internet-enabled multimedia system, thereby threatening the safety of the passengers [21–30]. Modern connected vehicles are susceptible to cyberattacks due to increasing connectivity, lack of secure network partitioning that

ensures separation of safety-related domains from the rest of the network, and lack of measures to verify the integrity and authenticity of Electronic Control Unit (ECU) software and communications [31]. On top of that, the communication architectures currently used in IVNs and the prevailing Controller Area Network (CAN) bus technology are inherently insecure and lack the necessary means of protecting against message tampering and spoofing attacks.

By virtue of the high regularity of the behavior of IVN messages and the well-defined specification of CAN communication, anomaly-based attack detection has been considered as a viable approach to detecting malicious traffic by monitoring for unlikely changes in the characteristics of CAN traffic.

1.2 Related Work

This section outlines the related work on process-level defense techniques tailored to cyber-physical systems. We discuss various approaches proposed by the research community, identify key fronts where the state-of-the-art solutions fall short, and state motivating challenges for this thesis.

1.2.1 Monitoring Cyber-Physical Systems (CPS)

Cyber-physical systems are a broad class of systems characterized by the interplay between cyber (virtual) elements and physical elements. What follows in a non-exhaustive account of research work related to this thesis on attack detection techniques for three types of CPS: control systems, smart grids, and connected vehicles.

1.2.1.1 Control Systems

Most existing approaches to detecting misbehaviors in the control of physical processes propose the use of model-based techniques to model the normal behavior of a process and then detect deviations therefrom [14, 18, 32–34]. While such approaches might prove viable in some cases where a detailed and complete specification of the physical process is at hand, in the real world, it is often the case that the system to monitor is fairly complex and lacks a roadmap to creating a model of the controlled process. Thus, building a

model of the physical process requires extensive human effort and domain knowledge, if at all possible [15].

Another disadvantage of model-based techniques lies in the fact that they involve solving a more general problem. Specifically, after presumably modeling the normal behavior of the process, the identified model is subsequently used to predict the future behavior of the underlying system, which is then compared to the observed behavior such that large deviations are labelled as potential attacks. Predicting the future behavior based on historical data is a more general problem than detecting the difference between past and current behaviors, and is known to be difficult and prone to inaccuracies due to noise in the data. Finally, since models are specific to the environments for which they were identified, model-based techniques prove difficult to generalize.

Approaches that use machine learning and data mining have been considered as well [13, 15, 35–39]. While machine learning methods do not require a model of the physical process, they involve a feature extraction and engineering phase, where *system-dependent* features need to be selected for training. Feature selection is tricky, hard to automate, and finding the best (most representative) features require a great deal of tuning and cross-validation. Moreover, the fact that features are constructed by combining various process variables and then transformed into high-dimensional feature spaces makes it difficult to identify the whereabouts of the attack and affects the interpretability of the detection results.

1.2.1.2 Smart Grid

Low-voltage distribution grids are witnessing a rapidly increasing integration of distributed inverter-based generation and thereby becoming subject to measurement falsification scenarios, wherein an adversary could corrupt voltage measurements received by so-called voltage droop controllers. Although inverters can participate in intelligent grid controls to solve voltage problems [40, 41], concerns have been raised about the impact of falsification attacks on system stability and voltage magnitude [42]. So-called cyber-secure modeling frameworks for the power grid and the communication networks have been proposed in [43, 44], as well as attack-detection algorithms for centralized voltage regulation [45] that are designed to detect attacks performed at the controller level only. A mo-

tivating challenge of part of this thesis was that no model-free anomaly-based detection techniques were identified in the literature that can monitor both controllers and actuators simultaneously.

1.2.1.3 Connected Vehicles

Modern connected vehicles are another type of cyber-physical systems that have attracted considerable attention from the cybersecurity community in light of the increasing attacks on vehicles. In recent years, there have been several attempts to design and develop anomaly-based intrusion detection systems for in-vehicle networks. Much of the related literature on in-vehicle attack detection lays particular emphasis on the well-defined specifications of CAN communication with respect to message periodicity and data content. The strict specifications of CAN communication have been leveraged in designing mitigation techniques that aim to detect non-compliant malicious communication [46–49]. In addition to leveraging the well-defined specifications of CAN communication, researchers have exploited the physical characteristics of CAN transceivers to develop attack- and source-detection techniques by fingerprinting ECUs [31, 50, 51].

Even though the state-of-the-art IVN intrusion detection systems are capable of detecting many types of attacks, they suffer from certain drawbacks, which served as motivating challenges for part of this thesis. In particular, most proposed methods require prior knowledge about the underlying IVN and ECU configurations, which may vary even in vehicles of the same model and year. Furthermore, with regards to coverage of different attacks, the proposed techniques have not been shown particularly capable of detecting attacks of a more stealthy nature.

In Section 1.4.1, we address the challenges and drawbacks of existing solutions by proposing a data-driven model-free technique that rather than creating a model to predict the future system behavior, directly compares the current behavior with the historical behavior of the process to detect changes in dynamics. Section 1.4.2 outlines our specification-agnostic approach for monitoring diverse and heterogeneous cyber-physical systems.

1.2.2 Deployment of Process-Aware Defenses

One of the motivating challenges for this thesis was to investigate the applicability and deployability of process-level intrusion detection systems in real and less-controlled environments to identify challenges pertaining to deployment, stability, and performance.

State-of-the-art process-level detection techniques have mainly been evaluated in simulation settings [52–54], on physical testbeds [16, 33], and on process data extracted from real environments [16, 35, 55]. Other related works proposed a hardware-based side-channel approach to process monitoring. For instance, Ahmed et al. [56] used noise patterns in sensor measurements, which appear due to manufacturing imperfections, to detect data integrity attacks while Van Aubel et al. [57] proposed to use electromagnetic measurements to detect behavioral changes in ICS software. However, to the best of our knowledge, there were no attempts in the literature to apply process-aware techniques on external sensors that can be added to sensitive parts of industrial machines to detect attack-induced abnormal changes in their dynamics. We outline our attempt in this regard as well as our approach to real-world evaluation in Section 1.4.3.

1.3 Research Questions

In this thesis, we study the cybersecurity landscape of modern cyber-physical systems and highlight their growing susceptibility to crippling attacks that have far-reaching consequences. We identify key research challenges in providing these systems with efficient and practical real-time detection capabilities that can alert operators of potential malicious schemes and thereby give them the opportunity to mitigate or minimize potential damage to safety-critical systems.

More specifically, this thesis identifies and contributes to the following research questions.

RQ1: How can a model-free approach significantly improve the accuracy and adaptability of process-aware defenses in industrial control environments?

RQ2: What theoretical and practical developments are needed for process-aware monitoring techniques to work across diverse cyber-physical systems and how can these be evaluated?

RQ3: To which extent are process-level monitoring solutions practical and applicable? What design and implementation challenges should be considered before deploying such research techniques in practice?

RQ1 is the core focus of this thesis as it relates to the fundamental problem of equipping safety-critical systems with adequate defensive means for combating malicious attempts that can have devastating impact on societies. Process-aware defense mechanisms are designed to capture the process dynamics from physics-based models of the process or from historical measurements that are representative of the process dynamics. Model-based techniques are hard to automate and require detailed specifications of the underlying process. By contrast, model-free techniques hardly require domain knowledge, can be significantly more accurate and noise-insensitive, and can be adapted to a wide range of systems. By proposing one such purely data-driven model-free technique with solid theoretical foundation and investigating its applicability to real-world problems, its generalizability to a broad class of complex systems of systems, and its deployability in real environments, we try to provide a roadmap for producing plausible security methods that have higher chances of being adopted by the industry.

RQ2 is relevant when one considers how diverse cyber-physical systems can be. For instance, pneumatic control systems, manufacturing robots, and modern vehicles are all cyber-physical systems, yet they differ widely in terms of architecture, system requirements, and operation. To appreciate this diversity, one may consider the plethora of cyber-physical "things" that are connected to the Internet and to open networks today. It is evident that designing security solutions that are specification-dependent may hinder their scalability. Therefore, it is an interesting challenge to develop techniques that can work across diverse cyber-physical systems.

RQ3 pertains to the hurdles that arise when moving research techniques from test labs to real environments. Since the ultimate goal behind research efforts is to produce technologies that can benefit society and the industry, it is imperative to investigate the

Table 1.1: A summary of how each chapter contributes to the research questions

	Part II Attack Detection in ICS		Part III Process-Aware Defenses for CPS			Part IV Deployment Challenges	
	Ch. 2	Ch. 3	Ch. 4	Ch. 5	Ch. 6	Ch. 7	Ch. 8
RQ1	●	●	●	●	●	●	●
RQ2	●	●	●	●	●	○	○
RQ3	○	○	○	○	○	●	●

challenges involved in the process in terms of viable deployment strategies, resource management, sustainability, and flexibility of operation under difficult conditions.

1.4 Thesis Contributions

This thesis contributes to the security of safety-critical cyber-physical systems by addressing the key challenges mentioned in Section 1.2 in view of the research questions stated in the previous section. Table 1.1 shows how each chapter relates to the research questions. Following is a summary of the contributions.

1.4.1 Process-Aware Detection Systems for ICS

In Part II of the thesis, we contribute to RQ1 by proposing a novel process-level detection technique and methodology for industrial control systems. We show the benefits of using a purely data-driven model-free approach that is inherently agnostic to the specifications of the monitored process. We also identify detection thresholds as a key parameter for this class of algorithms and propose a context-aware framework for a more sensible determination of this parameter.

(A) Departure-Based Detection of Stealthy Attacks

In Chapter 2, a novel ICS-specific intrusion detection method (PASAD) is introduced. PASAD is an anomaly-based process-level intrusion detection system that monitors ICS process activity in real time to determine whether the system operation is normal or

anomalous. Initially, PASAD learns the normal behavior recorded in a time series of sensor measurements through a training phase, during which ideas from a time-series analysis technique known as Singular Spectrum Analysis are applied to extract signal information from process output under normal conditions. Thereafter, the system continuously checks if incoming observations are departing from the normal behavior captured during the training phase.

PASAD is a theoretically sound, purely data-driven, lightweight, model-free mechanism that requires no prior knowledge of the system dynamics. Specifically, rather than creating a model of the physical process to predict future system behavior, PASAD seeks to solve the easier problem of deciding whether present sensor readings are departing from past readings due to a change in the mechanism generating them. Furthermore, by virtue of its impressive noise-reduction capabilities, PASAD is capable of detecting *slight variations* in the sensor signal. This leads to the possibility of detecting strategic attackers who may try to hide their stealthy attacks even at the process level. Finally, we show that PASAD compares favourably with state-of-the-art data-driven techniques and we demonstrate its effectiveness using a simulation platform, data from a physical testbed, and data from a real system.

(B) Robust Context-Aware Thresholds for CPS

In Chapter 3, we propose a context-aware framework for determining two-dimensional thresholds that enhance the sensibility and reliability of process-aware detection systems (PADS) by rendering them more robust to false detection. We argue that in the context of securing cyber-physical systems, relying on a single fixed threshold can undermine the effectiveness of the PADS as false alarms are highly costly for such systems that rely primarily on availability and continuity of operation. The proposed framework is context-aware as it takes into account the expected or typical reaction of a CPS to malicious manipulations in its operation and rests on two pillars: two-dimensional thresholds and actionability of alerts. Moreover, we present an algorithm that implements the concepts underlying our proposed framework. The algorithm implements two thresholds, raises both weak and actionable alerts according to which threshold is crossed, and the second threshold takes into account the typical score behaviour.

1.4.2 Process-Aware Detection Systems for CPS

In Part III of the thesis, we contribute to RQ1 and RQ2 by extending the operational capacity of our proposed detection technique to enable more scalability and make it applicable in various scenarios. We further apply our methodology on two representative cyber-physical systems: in-vehicle CAN networks and low-voltage distribution grids.

(C) Scalable Anomaly Detection in IIoT environments

In Chapter 4, we introduce M-PASAD, a multivariate extension of PASAD that can handle a plurality of sensors efficiently in IIoT cyber-physical environments. Although lightweight, fast, and suitable for distributed environments, the canonical way of monitoring n sensors simultaneously with PASAD at choke points is to awkwardly train and run n instances of the algorithm. Evidently, as the number of sensors grows large, the total time-to-train and allocated memory for deployment can quickly become overwhelming. The inevitable complexity and overhead involved in this approach is likely to hinder large-scale deployment of PASAD in industrial environments. Yet, with the monotonically increasing utilization of sensors, the scalability property is, at any rate, highly desirable. Rather than employing a plurality of PASAD instances, our proposed approach adapts the underlying theory to accommodate multiple sensors with little added complexity both in terms of running time and memory footprint. As such, M-PASAD inherits key features from PASAD, such as its noise-reduction potential, its capability to detect subtle structural changes in the monitored signal, and its efficient evaluation of the departure score during the detection phase.

(D) Detecting Attacks on In-Vehicle Networks

In Chapter 5, we investigate the applicability of our detection approach to an important emerging type of cyber-physical systems—the connected vehicle. We introduce a fast, lightweight, and specification-agnostic attack-detection mechanism for IVNs that goes a long way toward overcoming adoption hurdles imposed by the industry. We also demonstrate the effectiveness of our approach by conducting extensive experiments including performing stealthy attacks that we designed to serve as real-world scenarios on a 2018

Volvo XC60. Then we show that by monitoring CAN traffic in a way that treats the entire stream of CAN message payloads as a single signal we require no comprehension of the actual encoded signals and the underlying vehicle specifications that are typically proprietary. As such, our approach is applicable to vehicles of different brands and configurations. Finally, we demonstrate that by identifying malicious manipulations directly at the payload level PASAD is capable of detecting strategic adversaries who ensure that message frequencies and low-level ECU configurations remain intact under the attack.

(E) Detecting Attacks on Low-Voltage Distribution Grids

In Chapter 6, we investigate the applicability of process-aware detection systems to low-voltage distribution grids. Due to limitations, costs, and growing concerns over environmental impact of the electricity grid, transitioning into the envisioned cost-effective, more environment-friendly, highly manageable and controllable *smart grid* has become increasingly pressing over the past few years. The successful operation of smart grid services relies heavily on fine-grained smart meter readings. The transmission of such sensitive data over insecure communication links, however, goes beyond privacy issues and opens doors to malicious actors to compromise the grid operation via cyberattacks that could cause, for instance, a massive operational failure of energy assets. We investigate the effectiveness of PASAD in detecting various common types of cyberattacks on LV-grids. PASAD captures the dynamics of voltage-control loops by processing time series of controller and smart-meter data. The use of our model-free detection approach in current LV grids is motivated by the difficulty of modelling current distribution grids due to scarce and often inaccurate data, and by the fact that PASAD is inherently agnostic to the controller scenario and can thus be used for different kinds of control, independently of the underlying LV grid.

1.4.3 Deployment Challenges and Strategies

In Part IV of the thesis, we contribute to RQ3 by investigating the challenges of deploying process-level monitoring mechanisms in real environments as well as different deployment strategies.

(F) Deployment of PADS: The Nuts and Bolts

In Chapter 7, we investigate what it takes to deploy a PADS in a real ICS environment. The evaluation of ICS intrusion-detection methods in the literature seems to have been restricted to simulations and offline analysis of relevant datasets. In an attempt to bridge the existing simulation-based evaluation efforts with the real world by creating a roadmap characterizing potential hurdles to be expected when bringing the systems into a real environment, we take the evaluation of process-level monitoring a step further by running a fully fledged prototype in a real environment to examine the feasibility of the proposed methods in real-world settings. We build a complete system around PASAD, deploying a prototype in an operational paper factory, and describing our experience of running the prototype for 75 days. Finally, we highlight some technical challenges and practical aspects of live process-level monitoring for intrusions in ICS and then propose a set of guidelines and recommendations for both security researchers and practitioners who may consider designing or deploying IDS solutions for control systems.

(G) Deployment of PADS from a Side-Channel Perspective

In Chapter 8, we explore the viability of using PADS for side-channel based monitoring of industrial machinery. The principal idea is that industrial machines are poised to exhibit changes in physical properties, such as vibration and sound, when an attack is undergoing. As these properties can be measured with sensors, process-level attack-detection mechanisms may be used to detect such changes in behavior. Our side-channel based approach has the following merits: *i)* the detection system is relatively cheap and practical to deploy; *ii)* it is completely isolated, hence unreachable by the attacker; *iii)* and it makes fewer assumptions about data collection since it generates its own data. We tested our technique on an industrial metal lathe and a drilling machine and managed to successfully detect realistic attacks on them.

1.5 Conclusion and Future Work

In this thesis, we introduced approaches and techniques that contribute to the security and sustainability of modern cyber-physical systems. We have designed and thoroughly evaluated process-aware defenses, which are increasingly recognized as a modern security methodology for the highly connected industry.

The main contribution of this thesis is introducing a model-free process-aware attack-detection technique based on a novel time-series analysis methodology. The technique is lightweight, noise tolerant, and has been shown more capable than existing methods of detecting subtle changes caused by stealthy attacks. In addition, the thesis presented both theoretical and practical developments of the mentioned technique to make it scalable, adaptable to various system settings, and suitable for modern and emerging environments including IoT. Finally, the practicality of the process-aware detection technique was scrutinized in real-world settings to investigate its applicability and better understand deployment challenges.

As future work, interesting challenges to address include investigating how to properly handle alerts issued by the detection system in terms of up-streaming alerts to the operators, prompt reaction to a potential attack, and how to automate these procedures for systems that vary fundamentally in nature and mode of operation. It will also be interesting to identify the requirements for long-term deployment of process-aware defenses in industrial environments.

Bibliography

[1] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," *NIST special publication*, 2011.

[2] M. Allen and C. Pisani. (2018) Hacking and Cyber Warfare are Top Humanitarian Concerns. Last visited 2021-05-06. [Online]. Available: https://www.swissinfo.ch/eng/peter-maurer_hacking-and-cyber-warfare-are-top-humanitarian-concerns/43847744

[3] B. Gregory-Brown, "Securing Industrial Control Systems-2017," *SANS Institute InfoSec Reading Room*, 2017.

[4] N. Falliere, L. O. Murchu, and E. Chien, "W32. Stuxnet Dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[5] T. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, April 2011. [Online]. Available: https://openaccess.city.ac.uk/id/eprint/8203/

[6] L. Robert, M. Assante, and T. Conway, "German steel mill cyber attack," *SANS Industrial Control Systems*, vol. 30, p. 62, 2014. [Online]. Available: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[7] M. Abrams and J. Weiss, "Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia," *McLean, VA: The MITRE Corporation*, 2008.

[8] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer. (2017) Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. Last visited 2021-05-06. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[9] L. Robert, M. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems*, March 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[10] O. Vukmanovic and S. Jewkes. (2017) Suspected Russia-Backed Hackers Target Baltic Energy Networks. Last visited 2021-05-06. [Online]. Available: http://mobile.reuters.com/article/idUSKBN1871W5

[11] P. Polityuk, O. Vukmanovic, and S. Jewkes. (2017) Ukraine's Power Outage was a Cyber Attack: Ukrenergo. Last visited 2021-05-06. [Online]. Available: https://reut.rs/2mPSZqb

[12] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting the impact of stealthy attacks on industrial control systems," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 1092–1105. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978388

[13] M. Krotofil, J. Larson, and D. Gollmann, "The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '15. ACM, 2015.

[14] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 355–366. [Online]. Available: http://doi.acm.org/10.1145/1966913.1966959

[15] I. Kiss, B. Genge, and P. Haller, "A Clustering-Based Approach to Detect Cyber Attacks in Process Control Systems," in *Industrial Informatics (INDIN)*, 2015.

[16] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel, "Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ser. ACSAC '14. New York, NY, USA: ACM, 2014, pp. 126–135. [Online]. Available: http://doi.acm.org/10.1145/2664243.2664277

[17] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for Securing Cyber Physical Systems," in *Workshop on Future Directions in Cyber-physical Systems Security.* DHS, July 2009. [Online]. Available: http://chess.eecs.berkeley.edu/pubs/601.html

[18] Y. Liu, P. Ning, and M. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," *ACM Transactions on Information and System Security (TISSEC)*, 2011.

[19] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, Feb 1987.

[20] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," *Annales Des Télécommunications*, vol. 55, no. 7, pp. 361–378, Jul 2000. [Online]. Available: https://doi.org/10.1007/BF02994844

[21] A. Wright, "Hacking Cars," *Communications of the ACM*, vol. 54, no. 11, pp. 18–19, 2011.

[22] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Conference on Security*, ser. SEC'11. Berkeley, CA, USA: USENIX Association, 2011, pp. 6–6. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028067.2028073

[23] M. Zhao, J. Walker, and C.-C. Wang, "Challenges and Opportunities for Securing Intelligent Transportation System," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 96–105, 2013.

[24] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks," in *Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on.* IEEE, 2013, pp. 1–12.

[25] P. Kleberger, T. Olovsson, and E. Jonsson, "Security Aspects of the In-Vehicle Network in the Connected Car," in *2011 IEEE Intelligent Vehicles Symposium (IV)*, June 2011, pp. 528–533.

[26] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, and H. Shacham, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy.* IEEE, May 2010, pp. 447–462.

[27] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," *Black Hat USA*, 2015.

[28] F. Lambert. (2017) Keen Lab Hackers Managed to Take Control of Tesla Vehicles Again. Last visited 2021-05-06. [Online]. Available: https://electrek.co/2017/07/28/tesla-hack-keen-lab/

[29] K. S. Lab, "Experimental Security Assessment of BMW Cars: A Summary Report," Tech. Rep., 2018, last visited 2021-05-06. [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

[30] S. Nie, L. Liu, and Y. Du, "Free-Fall: Hacking Tesla from Wireless to CAN Bus," 2017, last visited 2021-05-06. [Online]. Available: https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf

[31] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *25th USENIX Security Symposium (USENIX Security 16).* Austin, TX: USENIX Association, 2016, pp. 911–927. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cho

[32] D. I. Urbina, D. I. Urbina, J. Giraldo, A. A. Cardenas, J. Valente, M. Faisal, N. O. Tippenhauer, J. Ruths, R. Candell, and H. Sandberg, *Survey and New Directions for Physics-Based Attack Detection in Control Systems*. US Department of Commerce, National Institute of Standards and Technology, 2016.

[33] A. Mathur and N. O. Tippenhauer, "SWaT: A Water Treatment Testbed for Research and Training on ICS Security," in *Cyber-physical Systems for Smart Water Networks (CySWater), 2016 International Workshop on*. IEEE, April 2016, pp. 31–36.

[34] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, "Unmanned Aircraft Capture and Control via GPS Spoofing," *Journal of Field Robotics*, 2014.

[35] C. Feng, T. Li, and D. Chana, "Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2017, pp. 261–272.

[36] P. Nader, P. Honeine, and P. Beauseroy, "Lp-Norms in One-Class Classification for Intrusion Detection in SCADA Systems," *IEEE Trans. Industrial Informatics*, vol. 10, no. 4, pp. 2308–2317, 2014.

[37] Y.-j. Xiao, W.-y. Xu, Z.-h. Jia, Z.-r. Ma, and D.-l. Qi, "NIPAD: A Non-Invasive Power-Based Anomaly Detection Scheme for Programmable Logic Controllers," *Frontiers of Information Technology & Electronic Engineering 18, 519–534*, 2017.

[38] K. N. Junejo and J. Goh, "Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning," in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*. ACM, 2016.

[39] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov 2015.

[40] P. Aristidou, G. Valverde, and T. Van Cutsem, "Contribution of Distribution Network Control to Voltage Stability: A Case Study," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 106–116, 2017.

[41] T. le Fevre Kristensen, R. L. Olsen, J. G. Rasmussen, and H.-P. Schwefel, "Information Access for Event-Driven Smart Grid Controllers," *Sustainable Energy, Grids and Networks*, vol. 13, pp. 78–92, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352467717301133

[42] M. Ma, A. M. Teixeira, J. van den Berg, and P. Palensky, "Voltage Control in Distributed Generation under Measurement Falsification Attacks**This work is sponsored by Chinese Scholarship Council (CSC)," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8379–8384, 2017, 20th IFAC World Congress. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405896317321547

[43] A. M. Giacomoni, S. M. Amin, and B. F. Wollenberg, "A Control and Communications Architecture for a Secure and Reconfigurable Power Distribution System: An Analysis and Case Study," in *18th IFAC World Congress, Milano, Italy*, 2011.

[44] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards Modelling the Impact of Cyber Attacks on a Smart Grid," *Int. J. Secur. Netw.*, vol. 6, no. 1, p. 2–13, Apr. 2011. [Online]. Available: https://doi.org/10.1504/IJSN.2011.039629

[45] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of Cyber Attacks against Voltage Control in Distribution Power Grids with PVs," *IEEE Transactions on Smart Grid*, 2016.

[46] M. Müter, A. Groll, and F. C. Freiling, "A Structured Approach to Anomaly Detection for In-Vehicle Networks," in *2010 Sixth International Conference on Information Assurance and Security (IAS)*. IEEE, Aug. 2010, pp. 92–98.

[47] M. Müter and N. Asaj, "Entropy-Based Anomaly Detection for In-Vehicle Networks," in *2011 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2011, pp. 1110–1115.

[48] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, "A Method of Preventing Unauthorized Data Transmission in Controller Area Network," in *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th.* IEEE, 2012, pp. 1–5.

[49] M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, and S. J. Prowell, "Modeling Inter-signal Arrival Times for Accurate Detection of CAN Bus Signal Injection Attacks: A Data-driven Approach to In-vehicle Intrusion Detection," in *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, ser. CISRC '17. New York, NY, USA: ACM, 2017, pp. 11:1–11:4. [Online]. Available: http://doi.acm.org.proxy.lib.chalmers.se/10.1145/3064814.3064816

[50] P.-S. Murvay and B. Groza, "Source Identification Using Signal Characteristics in Controller Area Networks," *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395–399, 2014.

[51] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee, "Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 4757–4770, June 2018.

[52] J. Downs and E. Vogel, "A plant-wide industrial process control problem," *Computers & Chemical Engineering*, vol. 17, pp. 245–255, 1993.

[53] R. D. Zimmerman, C. E. Murillo-Sánchez, and D. Gan, "MATPOWER: A MATLAB Power System Simulation Package," *Manual, Power Systems Engineering Research Center, Ithaca NY*, vol. 1, 1997.

[54] L. Rossman, "The EPANET Programmer's Toolkit for Analysis of Water Distribution Systems," in *WRPMD'99: Preparing for the 21st Century*, 1999, pp. 1–10.

[55] W. Aoudi, M. Iturbe, and M. Almgren, "Truth will out: Departure-based process-level detection of stealthy attacks on control systems," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, 2018. [Online]. Available: http://doi.acm.org/10.1145/3243734.3243781

[56] C. M. Ahmed, J. Zhou, and A. P. Mathur, "Noise Matters: Using Sensor and Process Noise Fingerprint to Detect Stealthy Cyber Attacks and Authenticate Sensors in CPS," in *Proceedings of the 34th Annual Computer Security Applications Conference*, ser. ACSAC '18. New York, NY, USA: ACM, 2018, pp. 566–581.

[57] P. Van Aubel, K. Papagiannopoulos, Ł. Chmielewski, and C. Doerr, "Side-channel based intrusion detection for industrial control systems," in *International Conference on Critical Information Infrastructures Security*. Springer, 2017, pp. 207–224.