

Linköping Studies in Science and Technology.
Licentiate Thesis No. 1881

A Timing Approach to Network-based Anomaly Detection for SCADA Systems

Chih-Yuan Lin

Linköping Studies in Science and Technology
Licentiate Thesis No. 1881

A Timing Approach to Network-based Anomaly Detection for SCADA Systems

Chih-Yuan Lin



Linköping University
Department of Computer and Information Science
Software and Systems
SE-581 83 Linköping, Sweden

Linköping 2020

This is a Swedish Licentiate's Thesis

Swedish postgraduate education leads to a doctor's degree and/or a licentiate's degree.

A doctor's degree comprises 240 ECTS credits (4 years of full-time studies).

A licentiate's degree comprises 120 ECTS credits.

Edition 1:1

© Chih-Yuan Lin, 2020

ISBN 978-91-7929-836-4

ISSN 0280-7971

URL <http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-165155>

Published articles have been reprinted with permission from the respective copyright holder.

Typeset using L^AT_EX

Printed by LiU-Tryck, Linköping 2020

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems control and monitor critical infrastructure in society, such as electricity transmission and distribution systems. Modern SCADA systems are increasingly adopting open architectures, protocols, and standards and being connected to the Internet to enable remote control. A boost in sophisticated attacks against SCADA systems makes SCADA security a pressing issue. An Intrusion Detection System (IDS) is a security countermeasure that monitors a network and tracks unauthenticated activities inside the network. Most commercial IDSs used in general IT systems are signature-based, by which an IDS compares the system behaviors with known attack patterns. Unfortunately, recent attacks against SCADA systems exploit zero-day vulnerabilities in SCADA devices which are undetectable by signature-based IDSs.

This thesis aims to enhance SCADA system monitoring by anomaly detection that models normal behaviors and finds deviations from the model. With anomaly detection, zero-day attacks are possible to detect. We focus on modeling the timing attributes of SCADA traffic for two reasons: (1) the timing regularity fits the automation nature of SCADA systems, and (2) the timing information (i.e., arrival time) of a packet is captured and sent by a network driver where an IDS is located. Hence, it's less prone to intentional manipulation by an attacker, compared to the payload of a packet.

This thesis first categorises SCADA traffic into two groups, request-response and spontaneous traffic, and studies data collected in three different protocol formats (Modbus, Siemens S7, and IEC-60870-5-104). The request-response traffic is generated by a polling mechanism. For this type of traffic, we model the inter-arrival times for each command and response pair with a statistical approach. Results presented in this thesis show that request-response traffic exists in several SCADA traffic sets collected from systems with different sizes and settings. The proposed statistical approach for request-response traffic can detect attacks having subtle changes in timing, such as a single packet insertion and TCP prediction for two of the three SCADA protocols studied.

The spontaneous traffic is generated by remote terminal units when they see significant changes in measurement values. For this type of traffic, we first use a pattern mining approach to find the timing characteristics of the data. Then, we model the suggested attributes with machine learning approaches and run it on traffic collected in a real power facility. We test our anomaly detection model with two types of attacks. One causes persistent anomalies and another only causes intermittent ones. Our anomaly detector exhibits a 100% detection rate with at most 0.5% false positive rate for the attacks with persistent anomalies. For the attacks with intermittent anomalies, we find our approach effective when (1) the anomalies last for a longer period (over 1 hour), or (2) the original traffic has relatively low volume.

This work has been supported by the Swedish Civil Contingencies Agency (MSB) through the RICS research center on Resilient Information and Control Systems (www.rics.se)

Acknowledgments

First, I want to thank my main supervisor Simin Nadjm-Tehrani for enabling this joint work between the Swedish Defense Research Agency (FOI) and Linköping University. Her support and mentorship provide helpful guidance on my research. I would also want to thank my co-supervisor Mikael Asplund for valuable discussions and suggestions throughout the work.

Thanks to Jonas Almroth, Erik Westring, and Peter Andersson in FOI, and other industrial partners for helping with data collection. Further, I'm grateful to all the administrative personnel, especially Anne and Lene, who make me capable of focusing on my research.

I would like to thank all the former and current members of RTSLAB for contributing to an enjoyable and inspiring working environment. I appreciate their valuable input to my research and presentations during the RTS meetings or fikas. Thanks to the SaS lunch group for providing relaxing breaks that are full of fun and useful life experiences.

Finally, I would like to express special thanks to my family and friends for encouragement and support in the past years. I would not have been able to get through the tough times without my husband Kue-Hsi's support and care. Love you!

Chih-Yuan Lin
Linköping, April 2020

Contents

Abstract	iii
Acknowledgments	v
Contents	vi
List of Figures	vii
1 Introduction	1
1.1 Background	3
1.2 SCADA cybersecurity countermeasures	6
1.3 Related work	11
1.4 Research questions	15
1.5 Contributions	17
1.6 Conclusions and Future Work	20
Bibliography	23
Paper A	35
Paper B	51
Paper C	73

List of Figures

1.1	A conceptual SCADA system architecture	3
1.2	A classification tree for intrusion detection techniques in SCADA systems	7



1

Introduction

Supervisory Control and Data Acquisition (SCADA) systems are used to control and monitor critical infrastructure such as power plants, water distribution facilities, and gas pipelines, etc. Historically, SCADA systems were composed by special-purpose embedded devices communicating through proprietary protocols in an isolated network. These legacy systems and devices were designed without cybersecurity concerns because of the closed operating environment. Over the years, SCADA systems are increasingly adapting to open protocols and standards and being connected to the Internet. The utilization of open protocols and standards improves interoperability between multi-vendor devices. The connection to the Internet allows distribution of SCADA functionality across a Wide Area Network (WAN) and remote control. However, these changes in communication technologies are accompanied by exposure of vulnerabilities in SCADA networks to the malicious attackers.

Due to the special characteristics of SCADA systems, many standard cybersecurity mechanisms are not properly implemented in SCADA systems. For example, legacy devices are kept and integrated into modern SCADA systems during the process of modernization. The legacy devices have limited computation ability for defense mechanisms that requires mass processing power such as encrypted communication. It's also quite common that these systems provide only weak authentication by using default passwords on the Commercial Off-The-Shelf (COTS) applications and devices. Some of the systems even use hardcoded passwords. One of the vulnerabilities

Stuxnet [34] worm exploited is a hardcoded password used in the Siemens WinCC product. However, patches and upgrades are not always available or applicable. Critical infrastructure and its control systems are vital to our daily life and, therefore, should not be subject to failures or shutdowns. Most patches and upgrades require the shutdown and restart of the controlling process. Some patches can also break the dependencies between components in a system (e.g., use the same hardcoded password everywhere).

Most experts agree *defense-in-depth* strategy is the best practice for SCADA system cybersecurity [61, 88]. This layered approach includes both preventative and detective technologies. Intrusion Detection Systems (IDS) are suggested for monitoring unusual and unauthorized activity in SCADA networks. Most of the commercial IDSs are signature-based. The vendors provide traffic signatures of attacks and the IDSs send alarms when finding traffic matching such signatures. Vulnerabilities and attacks in SCADA environments are very different from those in business environments. Infamous attacks such as Stuxnet and TRISIS¹ exploit zero-day vulnerabilities in SCADA devices. Since signature-based IDSs are not capable of detecting zero-day attacks, different approaches to form SCADA-specific IDS need to be explored.

This work aims to provide anomaly detection approaches in SCADA networks. Anomaly detection is a technique to model normality and identify deviations from the normality. It thus has the benefit of being able to detect previously unknown attacks (zero-day attacks). One of the main challenges of anomaly detection is the potentially large number of false positives coming from benign traffic that deviates from the trained normality due to the noise or environmental changes. However, compared with standard information and communication systems, SCADA systems exhibit more stable and regular communication patterns since the communications are triggered by programs to complete some repeated tasks. In addition, the network components and services in SCADA networks usually have long lifetimes and it is rare for SCADA networks to include new network components and start new services. These characteristics provide opportunities for anomaly detection.

In the following, we provide an overview of SCADA systems and SCADA cybersecurity in Section 1.1. Section 1.2 compares network-based anomaly detection with different approaches securing SCADA systems. Section 1.3 presents the related work. We discuss tackled research questions in Section 1.4 and our contributions to answer these questions in Section 1.5. Section 1.6 concludes this thesis overview and highlights the possible future work.

¹MAR-17-352-01 HatMan.
HatMan—Safety-System-Targeted-Malware

<https://www.us-cert.gov/ics/MAR-17-352-01-HatMan>

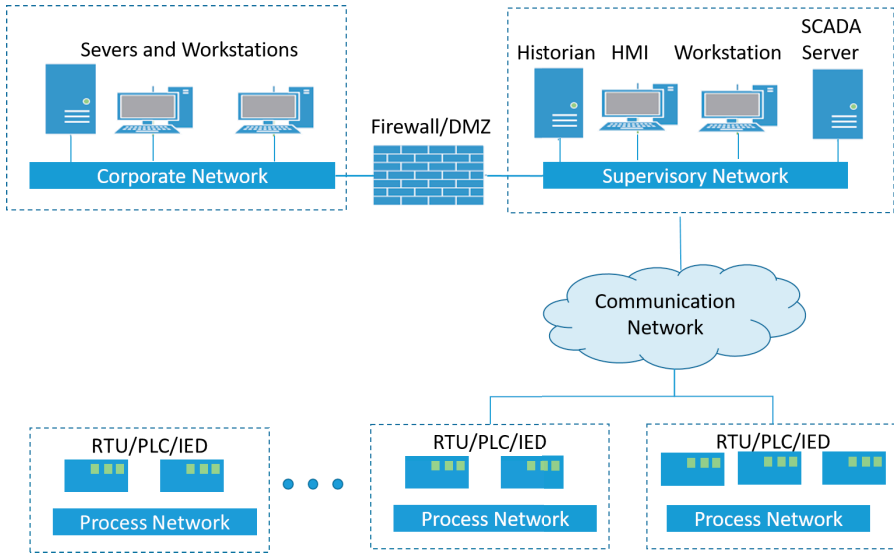


Figure 1.1: A conceptual SCADA system architecture

1.1 Background

This section first presents an overview of SCADA systems and introduces SCADA terminologies. Then it summarizes the trend of discovered vulnerabilities and important incidents in SCADA systems.

SCADA system overview

The details of SCADA system implementations may vary based upon the type and complexity of the controlled process, but there are some common components that can be found in a current SCADA system as illustrated in Figure 1.1.

1. Corporate network: A corporate network is a group of computers used in the office environment of the utility company, where the process information is stored, retrieved, and operated. It contains workstations for general users and some servers for IT management such as File Transfer Protocol (FTP) and mail servers. Though corporate networks are usually separated from the other part of SCADA systems with a firewall and demilitarized zone (DMZ), the increased connectivity poses security problems that were restricted in the corporate environment to the core of SCADA systems.
2. Supervisory network: The supervisory network resides in the control room. A SCADA server, or an Master Terminal Unit (MTU), is respon-

sible for issuing commands to and collecting, storing and processing data from field devices at the remote locations. Operators can access the graphical data and issue commands through an Human Machine Interface (HMI). Other common devices in a control room include Historian databases that the SCADA server can retrieve historical data from and engineering workstations that are used to configure the field devices in the remote locations.

3. Process network: The process network is formed by a group of field devices such as Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), and Intelligent Electronic Devices (IED) in the remote locations. The field devices are connected to sensors and actuators and store the value of monitored objects in device memory. Every monitored object can be represented as a (virtual) memory address. The field devices provide a communication interface to the SCADA server and these values can be retrieved and sent to the SCADA server later.
4. Communication network: The communication network connects the SCADA server and field devices. The communication is usually conducted through SCADA-specific protocols such as open standard protocols, Modbus [78], DNP3 [30], and IEC 60870-5-104 [50] (hereafter referred to as IEC-104). Some proprietary protocols such as Siemens S7 are also widely used. The communication between the SCADA server and the field devices is bidirectional, but most of the SCADA servers request data periodically through a polling program and receive corresponding responses from field devices later. This is called *request-response communication* in this thesis. Some SCADA protocols also allow *non-requested communication*, which means the field devices can send data without receiving any request. There are two types of non-requested communication: Some protocols enable configuring periodic communication events without requests and some protocols enable *spontaneous events*. In spontaneous communications, RTUs scan the device memory with a fixed rate and generate spontaneous events when the monitored data of the underlying process has changed (e.g., from 0 to 1) or fallen outside predefined ranges.

Each of these networks has different characteristics. The most suggested defensive approach is defense-in-depth, which secures each of them with multiple technologies (e.g., firewall, DMZ, IDS, etc.). In this thesis, we focus on the IDSs located on the communication network. Hereafter, we refer to a combination of supervisory network, process network, and communication network between them as a SCADA network.

SCADA vulnerabilities

SCADA systems are prone to various types of attacks due to lack of security controls. In the past, the SCADA devices were special-purpose embedded devices communicating through proprietary protocols and dedicated lines. Earlier system designers and critical assets owners believed that the SCADA systems were secure because of (1) *air gap*, (2) *security through obscurity*. The term *air gap* describes the fact that SCADA networks could be physically isolated from other networks and hence attackers could not access the SCADA networks. The *security through obscurity* means that there is very little information about the systems available to the public. The attackers could not easily learn and exploit the vulnerabilities. Therefore, these devices were designed to provide good performance with major concerns on task constraints such as real-time processing and jitter limitation. The security features were hardly included in the system design and development processes.

Over the last decades, some changes for the modernization of SCADA systems have been applied. The main changes are as follows: (1) Increased connectivity between the corporate network, supervisory network, and even process network for improved ease of use and remote accessibility. This makes the simple, isolated network into a complex inter-network. (2) Adoption of open standard protocols. This allows the interoperability between the devices from different vendors. (3) Use of COTS devices to reduce the design cost. Due to the use of COTS devices, a number of SCADA protocols are designed to operate on traditional Ethernet networks and the TCP/IP stack. These changes make the previous belief on the air gap and security through obscurity no longer true.

The legacy devices and COTS software are often not very secure. In 2016, Kaspersky Inc. published a review [5] that summarizes the vulnerabilities of SCADA devices according to the data from the United States Department of Homeland Security². The results show that the reported vulnerabilities in SCADA devices are growing. The discovered number of vulnerabilities grows from 5 in 2005, 19 in 2010, to 189 in 2015. Moreover, not all the vulnerabilities discovered in the previous years have been fixed (with patches or new firmware) by the time of publication.

Despite the increased connectivity between SCADA systems, the communications between these networks should be separated by firewalls and DMZ as shown in Figure 1.1. However, the separation of networks are not always properly set. TrendMicro Inc. published a security report in 2018 [47] and found numerous exposed HMI devices for different critical infrastructures including water systems, power systems, and gas and oil systems. These HMI devices are exposed on the Internet mostly because of inappropriate use of Remote Desktop Protocol or Virtual Network Computing.

²ICS-CERT. <https://ics-cert.us-cert.gov/>

SCADA threats

The number of attacks against SCADA networks grows as the number of vulnerabilities increases. Byres and Lowe [17] surveyed the attacks against SCADA networks maintained by the Industrial Security Incidents Database³ (updated until 2015). They found that before year 2000 almost 70% of the reported incidents were due to insiders, either with unintentional misbehaviors or with malicious actions. Since 2001, almost 70% of the incidents were due to attacks from outside the SCADA network. In addition to that, 86.8% of reported incidents happened after 2000.

More recently, more attacks targeted and tailored for specific SCADA systems were discovered. Stuxnet [34], discovered in 2010, was developed to target a specific type of PLC used in a uranium fuel enrichment plant in Natanz, Iran. Around 1,000 centrifuges were affected by Stuxnet. Duda [13], discovered in 2011, was similar to Stuxnet but it only collected data on the site silently. Since Duda removed its own components after a period of time, it was difficult to estimate the number of infected systems. Flame [4], discovered in 2012, infected Windows machines through two zero-day exploits. It was used to collect data through various interfaces including microphones, webcams, screenshots, etc. Irongate [48], targeting on Siemens PLC, was discovered in 2015 but considered as just a prototype, not yet an active malware. The Ukrainian capital Kiev was cut off the power supply by cyberattacks [62] at the end of 2015 and 2016 respectively. These attacks were complex with social engineering techniques and malware infections. The TRITON/TRISIS malware, which targets industrial safety systems and intends to cause physical destruction, attacked a Saudi Arabian petrochemical facility in 2017. In 2018, the U.S. Department of Homeland Security and FBI released official alerts⁴ on a series of a multi-stage intrusion campaign targeting energy and other critical infrastructure sectors. The attack continued into 2019.

1.2 SCADA cybersecurity countermeasures

This section provides an overview of SCADA cybersecurity countermeasures with a focus on IDSs for SCADA systems and how the other countermeasures are related to IDSs. We first classify the IDSs into categories and introduce each group of IDSs in comparison with each other. Then, we position IDSs to a bigger picture of SCADA security and elaborate how IDSs fit in the bigger picture and complement other security countermeasures.

³RISI. <https://www.risidata.com/>

⁴TA18-074A. <https://www.us-cert.gov/ncas/alerts/TA18-074A>

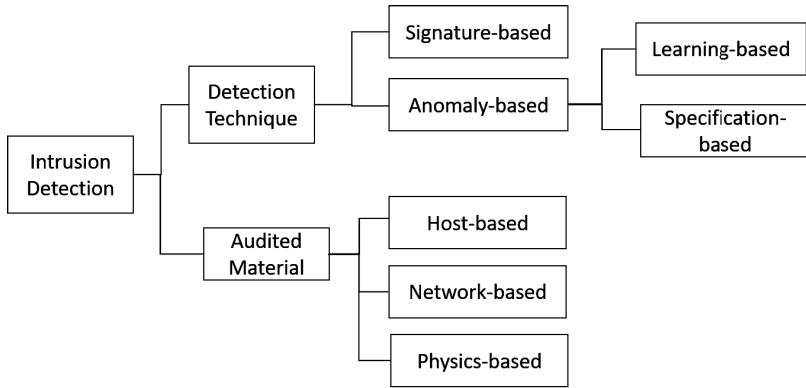


Figure 1.2: A classification tree for intrusion detection techniques in SCADA systems

SCADA IDS classification

Intrusion detection systems (IDS) have been widely regarded as an important means to prevent unauthorized access to SCADA systems. One of the most common taxonomies of IDSs is based on two classification dimensions *detection technique* and *audited material* [76, 49] as illustrated in Figure 1.2.

The detection technique item classifies the intrusion detection techniques into signature-based systems and anomaly-based.

Signature-based (or knowledge-based) systems look for specific patterns of misbehavior. Most of the commercial IDSs are signature-based. To run this kind of IDSs, there must be a group of experts analyzing attacks and finding the patterns of attacks. The patterns are then transformed into rules of an IDS. The IDS compares the system's behavior and the patterns in runtime, and it's considered as an intrusion when a pattern is matched. Most commercial IDSs are not capable of monitoring SCADA systems due to lack of understanding of the SCADA-specific protocols and attacks. Therefore, the research on this area mostly focuses on analyzing attack patterns and transforming them into rules that can be deployed in a current platform [81, 94]. These systems have high accuracy on known attacks and low false positive rates (FPR) but cannot detect zero-day attacks.

Anomaly-based (or behavior-based) systems look for deviations from the ordinary behaviors and thus are capable to identify unknown attacks (i.e., zero-day attacks). The main disadvantage of such systems in general IT networks is the susceptibility to false positives. Anomaly-based IDSs need to create a model of ordinary behaviors and the steady nature of SCADA systems creates new opportunities for anomaly-based IDSs. SCADA networks are much more stable and regular than IT networks in terms of network architecture and communications.

We can further distinguish these IDSs into learning-based and specification-based systems. A **learning-based** approach builds its model by learning from historical data. It doesn't have to be a machine learning process but can be a simple statistics calculation. The main advantage of learning-based approaches is generality that the same process can be applied to different SCADA networks as long as they have similar behaviors. A **specification-based** approach in the other way creates its model directly from the specification of the system. The specification can be a protocol specification, a system configuration, or any description of the system without a learning process. Therefore, it is easy to find which specification rule caused the alerts. However, specification-based approaches usually require manual analysis of the documentation when applying to a new system.

The audited material item in Figure 1.2 classifies the intrusion detection techniques into network-based, host-based, and physics-based systems.

Host-based systems monitor the behavior of specific nodes by the logs, procedures (e.g., runtime stack), and keystroke data, etc. They identify misbehavior in node/component levels and enable distributed control. This is attractive for more advanced critical infrastructure such as smart grids. Another advantage of host-based IDSs is the ability to identify the nodes under attack. However, the requirement of resources on the end nodes for data storage and computations makes them less applicable to a SCADA network with legacy devices.

Network-based systems model and analyze network communication attributes. Using network data allows end nodes to be free from maintaining system logs or complicated computations, but it may be hard to identify which nodes/components are under attack. Most of the proposed IDSs in SCADA systems are network-based [76]. Network-based IDSs have potential to block attacks before they arrive at field devices or important hosts if the security manager responds to warnings with a preventive technology such as firewall. This domain can be divided into several main strains by the used features of the data. Some research focuses on throughput, some on timing, and some on payload of packets. Our work is network-based with a focus on timing, and we discuss the differences between each method in the related work section.

Physics-based (or semantic-based, process-aware) systems monitor the input/output values of one or multiple physical devices. The audited material can be signals from the sensors and actuators, measurement values from a network packet, or a combination of them. In early studies, physics-based approaches are not categorized as a group. These approaches are separately classified into network-based or host-based groups according to where they collect their data (from a device IO port or a network packet). Recently, more research has focused this group of IDSs and consider it as an independent strain of works [43]. physics-based IDSs use process variables to model a process that follows certain physical theory such as control theory. These

systems can accurately model the real-world system and estimate the trend of process variables, and therefore detect events driving the system into an unsafe state. The main disadvantage of physics-based IDSs is late detection. These systems detect an attack or undesired activity only when it arrives at the physical devices or impacts the process which may lead to safety issues in the context of critical infrastructure.

Other countermeasures

The best practice to secure SCADA systems is defense-in-depth in which multiple security mechanisms are applied to protect the assets in the system. Defense-in-depth for SCADA systems combines a wide variety of security elements including risk management, physical security, human factors, and network monitoring. This subsection discusses technical methods proposed for SCADA systems and how these methods complement each other. That is, physical (e.g., fences and locks) and administrative (e.g., security policies and training) security methods are not included in this discussion though they are as important as the technical ones. Since the discussion focuses on emerging research topics, general and matured technologies such as firewalls and DMZ are not part of it as well.

Risk management. A defense-in-depth approach usually starts with risk management by which the system administrator can assess risks and decide how to treat different types of risks. Risk management is a continuous process to reduce risks of a system. The details of the process are slightly different under different contexts, but there are four common steps: identification, assessment, reduction, and monitoring [16].

1. Risk identification: In this step an organization needs to identify the risks by studying the threats and vulnerabilities of SCADA systems.
2. Risk assessment: The organization needs to estimate the potential impact of a threat or vulnerabilities through a risk assessment process. Generally speaking, risk is a function of the likelihood of a given threat exploiting a vulnerability and the criticality level of successful exploitation of the vulnerability. When assessing risks, it is important to take into consideration the impact on the physical devices and processes, and safety.
3. Risk reduction: According to the result of risk assessment, the organization applies different security controls such as IDSs and firewalls for risk reduction or mitigation.
4. Monitoring: Last but not least, the organization monitors and adjusts its security controls by gathering information through automated or manual process.

Cherdantseva et al. [26] conducted a review of twenty-four risk assessment methodologies for SCADA systems. Some of the works proposed a holistic approach including identification, assessment, reduction, and monitoring, but most of them focus on the risk identification and assessment step.

Traditionally, risk management is a manual process through a standardized framework [87]. The four steps of risk management are conducted sequentially and statically. In the past decade, people have combined risk assessment with real-time monitoring to address Advanced Persistent Threat (APT) problems [41, 79]. The four steps are conducted simultaneously and the real-time monitoring results become an input to risk assessment dynamically. In this strain of works, IDS is one of the common tools for real-time monitoring.

Forensics. Forensics is a technique for post analysis of an incident. When a system is compromised and an intrusion has been detected, there's a need for a forensics investigation to come in. The forensics investigation needs to collect evidence of the intrusion with regards to 6 Ws (who, what, when, where, why, and how) so that the intruder can be brought to justice.

According to the white paper by EU Cybersecurity Agency [84] SCADA forensics is defined in five steps: (1) examination of the system for the possible sources of evidence, (2) identification of the impact components, (3) collection of raw data, (4) analysis of evidence, and (5) documentation. Awad et al. [9] reviewed tools, techniques, and methodologies of SCADA forensics. Iqbal et al. [51] summarized the challenges in each step for SCADA forensics.

One of the main challenges in SCADA forensics is to collect evidence without impacting the function of the system. That is, due to the requirement of availability of SCADA devices, the analysis usually needs to be live forensics for SCADA systems. For the network analysis in live forensics, IDSs can be used to log information, such as time, source IP, and standard attack name [91]. IDSs also provide opportunities to find evidence of the next steps of an intrusion.

Attestation. Attestation is a procedure for an external entity (verifier) to verify the integrity of a system or a device (prover). The verifier sends a challenge to the prover, and it replies with a report. If the integrity of the prover has been tampered with, the reported results will be incorrect or there will be a noticeable increase in computation time. Traditionally, attestation mechanisms are static meaning that they verify the code integrity or loaded software of a device to assure there's no malware installed [25, 75]. Resource constraints in legacy devices and real-time requirements of SCADA systems are the main challenges. For example, phaser measurement units require message delivery within 20ms in a 50HZ power grid. The execution of attestation needs to be short enough to avoid impacting the normal service.

Recent efforts in SCADA attestation focus on defense against runtime attacks, for example, PAtt [42], which is a system that assures the control logic in runtime. The most common approach is to encode the execution path of

a process as a single hash or other representative forms. In order to monitor internal states of the control logic at runtime, PAtt takes sensor readings for physical process to authenticate the control logic hash. The procedure is similar to what a physics-based intrusion detection system does. Nonetheless, physics-based IDSs usually collect more information and model complicated systems, while providing only best-effort intrusion detection. In other words, an attestation approach provides higher level of assurance but it mostly works on embedded devices with information of execution path or control logic.

Honeypot. Honeypots are computer systems deployed to attract attackers in order to collect information from them. Conpot⁵ is a low-interactive SCADA honeypot that aims at easy deployment and modification. Most SCADA honeypots are used for information gathering that helps us understand current threats in the wild and discover potential attacks such as new botnets and viruses. The information collected by honeypots can be used for generation of attack patterns used by signature-based IDS [92, 59]. It's also possible to integrate a honeypot into an IDS [93].

Back to IDS. An IDS is a system monitoring tool. Solely monitoring can not prevent a system from cybersecurity incidents, but monitoring plays a key role for security managers to understand what's going on in the system during runtime and provides chances to reduce risks of APT or collect evidence of an intruder (and stop them in the real world). A combination of IDSs and other technologies, such as honeypot, can further increase the possibility to find out unknown attacks.

1.3 Related work

This section reviews related work in network-based and physics-based anomaly detection domain.

Network-based anomaly detection

This thesis contributes to network-based anomaly detection for SCADA systems. One of the reasons to choose network-based anomaly detection approaches is the stability of SCADA traffic. Compared to traditional IT traffic, the SCADA traffic usually exhibits stable characteristics with regards to its throughput, availability [37], and long TCP flow duration [10]. SCADA systems also have limited external access meaning that SCADA hosts and services are rarely added to or removed from the network [12]. Another reason to adopt anomaly detection approaches is the presence of zero-day exploits. Many known SCADA threats make use of zero-day exploits [34, 13, 4]. As

⁵<http://conpot.org/>

presented in Figure 1.2, there are two common approaches to form the ordinary behaviors for anomaly detection in SCADA networks, specification-based and learning-based approaches.

Specification approaches

Several papers confirm the feasibility of specification-based IDSs. Cheung et al. [27] model the Modbus TCP traffic based on the valid function codes of depend field. Garitano et al. [39] propose an algorithm to generate detection rules based on the description of the application with regards to its (1) number of variables, (2) class of variables, and (3) variable update rates. Lin et al. [66] model the DNP3 traffic and Yang et al. [98, 97] model the IEC-104 traffic based on the protocol specification analysis. Caselli et al. [21] propose a specification mining technique to automatically generate the specification rules from documentation about monitored systems and Esquivel-Vargas et al. [32] test such an IDS in A Data Communication Protocol for Building Automation and Control Networks (BACnet).

Learning approaches

A learning-based approach derives a behavior model by learning and the learning process may be able to be used in different SCADA networks. Different kinds of learning-based models have been suggested for SCADA-specific IDSs.

IDSs that leverage the overall network attributes such as throughput, number of protocols, bytes per packet are an active research area. These IDSs usually adopt *statistical models* [90, 14, 89] or *machine learning techniques* [70, 69, 67, 68, 71, 36, 6] and test if the value of the selected parameters of the model is within certain boundaries. Values within the boundaries give a high probability to be a normal behavior. These systems have been shown to be capable of detecting flooding like attacks (e.g., DDoS, SYN-flooding) through monitoring the collective network attributes. However, they provide little insights about which packets caused the anomalies and may not be able to detect sophisticated attacks having fewer changes in the overall network attributes.

To enhance the detection ability for more attack types, IDSs exploiting payload features have been proposed. Language models such as n -grams are widely used for both general purpose networks and SCADA networks. Bigham et al. [15] propose an anomaly detector which is a combination of a n -gram model and an invariant model of measurements that flow through the systems (i.e., constant relationships between measurements such as linear relationship). In the consecutive work of Jin et al. [52], the authors extend the invariant model by a value range model that allows values to vary between a predefined range. Düssel et al. [31] present an anomaly detection

system based on n -grams to calculate the distance of transport-layer packet payloads in the format of byte sequences. Hadžiosmanović et al. [45] and Wressnegger et al. [95] investigate n -gram analysis for message payloads of binary protocols. These approaches model the payload messages with their statistical attributes such as frequencies and probability of occurrences without understanding the SCADA specific content, some of them even model the payload in a binary format.

On the other hand, significant research efforts have been devoted to IDSs that require some prior knowledge of SCADA protocol and systems. These systems focus on traffic characteristics in a specific type of SCADA traffic such as timing patterns of certain types of commands. One of the most common hypotheses is that traffic created by request-response communications is highly periodic and contains well-defined message sequences. In the work by Sayegh et al. [85], the IDS models the time intervals between signatures (i.e., a sequence of packets) and calculates the rank of the transition probability for each packet after observing certain signatures that it is correlated with. Barbosa et al. [11] model the historical period of repeated messages in an orderless group. Sequence-aware intrusion detection systems employing *automata models* such as Deterministic Finite Automata (DFA) and Probabilistic Automata (PA) have been widely researched. Goldenberg and Wool [44], Faisal et al. [33], and Markman et al. [72] use DFA to model the message sequences of Modbus TCP traffic. Kleinmann and Wool [57, 56, 58] use DFA to model the message sequences for the Siemens S7 protocol. Casselli et al. [22, 23] model the message sequences of Modbus, MMS and IEC-104 traffic with Discrete-time Markov chain (DTMC). Yoon et al. [99] model the message sequences of Modbus as Dynamic Bayesian Network (DBN). These approaches are able to parse the application layer content of SCADA specific protocols and extract desired type of packets such as certain commands and responses. With the information from the application layer, the alarms can be identified by the node which sends the packet, instruction (e.g., command and request of data) of the packet, and even the memory address that the command/request is sending to or from. The semantic of the nodes, instructions, and memory addresses are usually well-defined in a SCADA system. Therefore, these approaches provide more insights about what happened in the system with the appearance of an alarm.

Most of the models in the previous paragraph makes use of Modbus traffic regularity. This thesis focuses on traffic characteristics of IEC-60870-5-104, which is recognized as an international standard of SCADA data transmission for electric utilities [29] and predominantly used in the European electrical industry. Compared with the the request-response mechanism used by Modbus protocol, IEC-104 protocol is more complicated. IEC-104 allows not only request-response communication, but also spontaneous communication. The work starts with the common hypothesis of request-response communications. Then we extend our knowledge of SCADA traffic to spon-

taneous communications by studying their traffic patterns and propose potential solutions to anomaly detection of IEC-104 non-requested traffic.

Physics-based anomaly detection

This thesis models SCADA traffic in both request-response communication and spontaneous communication modes. As mentioned in Section 1.1, the spontaneous traffic is generated by the RTUs when the monitored data of the underlying process changes. Physics-based IDSs that model the process with its sensor measurements and input commands are complementary to this thesis.

Some early studies propose specification-based IDSs. There are two types of specifications used for intrusion detection: critical states [19, 38, 18] and behaviour rules. Critical states document the conditions of process components that may cause safety issues. For example, a system may come into a critical state when its centrifuge rotates at less than 1000 rpm and its temperature is higher than 100 degrees Celsius. Behavior rules document the specifications of physical devices such as the radio range of the radio transmission component [77, 83]. The behaviour rules can also be conducted by physical laws such as $P = V \times I$ (P stands for power, V stands for voltage, and I stands for current) [28, 54].

The specification approaches require experts' involvement in the development process or detailed understanding of the system that are not always available. Therefore, specification-agnostic techniques have been considered. Recently, Khalili et al. [8] and Farsi et al. [35] study learning approaches to stated-based anomaly detection without manual critical state analysis. Their approaches identify and extract normal states to detect anomalies.

Most of the physics-based anomaly detection systems rely on a prediction of process behaviors. *System identification* can be used to learn the model of how a physical system behaves. Giraldo et al. [43] present a systematic review of physics-based attack detection in control systems. There are two popular methods used in the surveyed papers: Auto-Regression (AR) and Linear Dynamical State-Space (LDS). Hadžiosmanović et al. [46] use the AR technique together with Shewart control limits to model the process variable dynamics of operational water treatment plants. Shoukry et al.[86] use the LDS technique together with χ^2 statistics to build a physical challenge-response authentication method for active sensors. Cárdenas et al. [20] use the LDS technique together with a non-parametric cumulative sum statistics for anomaly detection. Additionally, Ahmed et al. [1, 2] adopt a subspace system identification method to identify linear time invariant models and create sensor fingerprints for anomaly detection.

Various known machine learning [80, 55, 60, 53, 96, 7, 40] and data mining [82] techniques have been used in physics-based anomaly detection as well. These approaches require no prior knowledge of the physical pro-

cess, but a certain amount of tuning and cross validation for feature selection. Among these works, clustering techniques used for anomaly detection on sensor measurements are noticeable. Krotofil et al. [60] adopt an information-theoretic approach to form clusters of correlated sensors. The authors build correlation entropy in clusters of related sensors to detect sensor signal manipulations. Kiss et al. [55] adopt the Gaussian mixture model to form sensor clusters and show that their approach outperforms the k-means clustering approach under the proposed experimental environment. Aoudi et al. [7] propose a departure-based detection system that measures the distance between the normal signals and the signals under attack. These works suggest that sensor measurements in a physical process are intricately correlated. Since the sensor values and spontaneous events have a cause-effect relationship, these works explain and support our hypothesis used for anomaly detection in spontaneous traffic: spontaneous traffic from different flows can be correlated.

1.4 Research questions

Our goal is to model the SCADA traffic for anomaly detection. The main challenge in anomaly detection is to find a robust modeling method that avoids a large number of false positives and has high accuracy. To achieve this level of robustness, the model used for anomaly detection must capture stable and persistent characteristics of SCADA traffic. Therefore, our research questions are:

RQ 1: Are there structural characteristics of SCADA traffic that can be used for an building anomaly detector? If so, how can we identify them? (paper A and B)

Awareness of traffic patterns in SCADA systems has increased since the publication of two papers by Cheung et al [27, 90]. The authors proposed two widely used hypotheses of SCADA traffic patterns, the regularity of request-response traffic and stability of network components, by manual observations on how SCADA systems running Modbus protocol work. The two hypotheses are in later works applied to anomaly detection for different SCADA networks running different protocols as mentioned in Section 1.3. Among them, some research shows that SCADA traffic contains perfect periodicity of messages, while some SCADA traffic cannot be well-modelled with the request-response regularity hypothesis [22, 23, 57].

In the past decade, machine learning techniques have been widely used in the general anomaly detection and intrusion detection area [24]. Thanks to advances in the machine learning area, it's now much easier to apply machine learning techniques on SCADA traffic that cannot be modeled by the request-response regularity and to find new characteristics that can be used for anomaly detection. The question is, what methods should we use?

In paper A, we collect datasets from different settings and with different SCADA protocols, model their periodicity and identify the source of non-periodic traffic. The most common non-periodic traffic is the spontaneous communication traffic. Spontaneous events are generated when the RTUs observe changes of value on the monitored objects. The changes can only be caused by the process subject to control if not manually set by an operator. We expect that the underlying control loop for the physical process presents some repeated behaviors in order to complete its regular workflow and the repeated behaviors lead to certain timing patterns in the spontaneous event sequences.

To confirm this speculation, we need to adopt sequential pattern mining techniques on the spontaneous event inter-arrival time sequences and observe whether there is any pattern that could last over time. If we can find sequential patterns of spontaneous event inter-arrival times $T = t_1, t_2, \dots, t_n$, we can predict the next event inter-arrival time element by looking into the historical inter-arrival time sequences. Consequently, we can predict when is the next event likely to come.

To model a sequential pattern, one would adopt a fixed order Markov Chain, which predicts the probability of the next element by looking into the previous m elements. However, it is difficult to decide the m during an learning process. A Variable-Length Markov Chain (VLMC) is a more suitable model. A VLMC can be efficiently stored and processed by a Probabilistic Suffix Tree (PST). A PST is a tree structure that learns a set of subsequences of different lengths and stores the number of occurrences of each subsequence in the leaves. The tree structure allows us to calculate the probability of the next element in an efficient way, and then make a prediction on the next element based on the learned elements with the highest probability. Since the process environment and network traffic are sometimes noisy and this leads to an increased number of nodes and links in the model, paper B uses PST to represent VLMC models.

RQ 2: How can we model the given structural characteristics for anomaly detection? (paper A and C)

Model the request-response traffic. With the given hypothesis of periodicity, there are two types of approaches: timing approaches and sequence approaches. Timing approaches model the relative timings between different packets or events (i.e., a certain command or measurement values from a certain memory address), and sequence approaches model the order of them.

Sequence models are not able to detect changes in timing without changes in the order of messages, but changes in the order of messages must impact their timing because some messages are promoted to the earlier position and some others are postponed. Unfortunately, at the time this work was started, the proposed timing models still suffered from high false positive rates. The proposed models, therefore, need to set a relaxed threshold for anomalies and cannot detect subtle changes in timing. So the question posed is: can

we find a better modeling method for the timing attributes? In paper A, we propose a timing-based model that can detect subtle changes in timing if the traffic is generated from a request-response communication mode.

Model the spontaneous traffic. With the traffic characteristics found in paper B, paper C makes two hypotheses for spontaneous traffic: limited groups of event inter-arrival times and correlations between flows. That is, a flow may have only a few possible ranges of inter-arrival times (e.g., 1-3, 5-7). Additionally, When the number of events in a flow decreases, the number of events in some other flows also decreases and vice versa.

For the inter-arrival time part, paper C proposes an algorithm to learn and estimate the ranges that are likely to happen for anomaly detection. Then the proposed anomaly detector shouts when seeing inter-arrival times falling outside all of the ranges. Paper C compares two estimation methods: best-fitting with percentile 99.99% historical inter-arrival times, and estimation with Gaussian distribution and three sigma rules.

For the correlation part, one could cluster all the flows in the format of event volume time-series during the learning time, and shout when the structure of clusters changed in runtime (e.g., one flow jumps from one cluster to another). In this method, the choice of cutoff line of correlation coefficients as a parameter has a huge impact on the clustering results and it's difficult to decide during the learning process. Therefore, paper C models correlations in pairs. Every flow is paired to its most-correlated flow and every pair has its own model of the relation. The proposed anomaly detector in paper C shouts when there is a relation break.

1.5 Contributions

This section summarizes the appended papers and states the contributions of each paper.

Timing-Based Anomaly Detection in SCADA Networks (Paper A)

This paper aims to leverage traffic periodicity for anomaly detection in SCADA networks. It models event inter-arrival time with sampling distribution of the sample mean and sample range and tests the approach with datasets from Siemens S7, Modbus, and IEC-104 networks. The tests are performed in the settings of three different attacks, flooding, single message injection, and TCP sequence prediction. These attacks are composed of valid messages so they cannot be detected by whitelisting mechanisms. Signature-based rules to identify any of these attacks is very hard if not impossible. The single message injection and TCP sequence prediction generate little change on the overall traffic attributes so it is hard to be detected by an IDS that monitors the overall network characteristics. The results in paper A show that the proposed approach can detect attacks with high accuracy and

low false positive rates for request-response communication traffic. With the non-requested communication traffic, the proposed approach leads to a large number of false positives.

Contributions. Using three different sources of data, this paper confirms a common hypothesis that request-response traffic in SCADA networks is highly periodic. With the request-response communication traffic, our approach successfully detects flooding attacks and the attacks that only cause subtle changes in inter-arrival periods (single message injection and TCP sequence prediction) with high accuracy and FPRs around 1%. To our knowledge, there is no SCADA-specific IDS that has successfully detected the TCP sequence prediction before the publication of paper A. In addition, this paper identifies the limitation of relying only on model traffic periodicity. The spontaneous events in the non-requested communications do not always generate periodic messages and thus cannot be modeled by their periodicity.

Understanding IEC-60870-5-104 Traffic Patterns in SCADA Networks (Paper B)

Paper B adopts pattern mining techniques based on PST to characterize IEC-104 spontaneous traffic generated by the non-requested communication mode. This paper provides a detailed analysis of how the spontaneous traffic flows between SCADA components with regards to its timing predictability and phase transitions. It proposes a modeling method based upon PST to discover the underlying event inter-arrival time patterns in the format of sequences. In 11 out of 14 emulated traffic flows created by a research testbed, RICS-el[3], we see evidence of the existence of the identified sequential patterns. With the patterns, the PST model can be used to predict when will the next spontaneous event come. Our approach shows an 80% prediction possibility for the best case, but most of the sequential patterns only enable moderate (40%-60%) prediction accuracy.

As observed in earlier works [44, 58, 73], SCADA traffic sometimes contains phase transitions and some of the attributes may change together with the phase transitions. We study the 14 traffic flows with regards to how their sequential patterns change over time and categorize five groups of behaviours: strongly cyclic, weakly cyclic, stable, and transitional. With a proposed definition of phase transition, this paper studies what is the impact of phase transitions on sequential patterns and how long does a phase last in the transitional group. In some of the cases, the prediction accuracy significantly decreases after a phase transition.

Contributions. This paper provides a novel approach to model and predict the timing of spontaneous traffic based on observations of past traffic. It indicates that timing predictability based on sequence patterns works but not on every flow. One of the possible reasons is that our learning period (2-

hours) is too short. In some cases, re-learning after phase transitions should also help.

The results extend our understanding of SCADA traffic and provide a first look at the network characteristics of IEC-104 spontaneous traffic. To our knowledge, this is the first study to characterize the spontaneous traffic in SCADA network. With two emulated IEC-104 datasets, it shows the timing of spontaneous traffic can be potentially used for anomaly detection. However, the phase transition analysis demonstrates that some attributes (inter-arrival time sequences) may change over phases and indicates the need for more studies on phase transitions.

Modeling IEC-60870-5-104 Spontaneous Events for Anomaly Detection (Paper C)

This paper proposes an anomaly detection system that combines two methods for modeling valid event inter-arrival times and the correlation between flows for IEC-104 spontaneous traffic. Based on the results of paper B, we propose two hypotheses about spontaneous traffic characteristics: limited group of inter-arrival times and correlation between flows. First, despite the fact that spontaneous event inter-arrival time sequences may not be regular enough for anomaly detection with methods like mean-range (paper A), the set of possible inter-arrival times may be relatively stable. Consequently, instead of finding the element with the highest probability and predicting the timing, the detector can find the elements that are not in the learned set or found with extremely low probability, and send alarms when these occur. Second, paper B categorizes the test data into five groups. Flows in the same group show changes in sequential patterns at approximately the same. This suggest that the underlying sequence patterns may change over time due to many reasons but some flows tend to change together. That is, there may exist a positive correlation between traffic flows in the same network. Based on this observation, paper C clusters the flows in the same system based on their correlation during learning time and at runtime considers the inter-arrival pattern that deviates from the correlated flow(s) as an anomaly.

The proposed detector is tested with datasets from a real power utility. Paper C also implement an attack simulator to simulate the impact of attacks on the original traffic. The tests are conducted in two attack scenarios: attack against field devices and malware inside field devices. In the first scenario, the attacker takes control of other devices in the network and launches attacks such as packet flooding against a field device. The attack packets compete for resources on the field device with the normal packets and might cause performance degradation. In the second scenario, the attacker exploits field device vulnerabilities and tries to damage the controlled process. In order to hide its malicious activities, the malware might suppress the real outbound packets and sends forged packets with contents recorded

in the previous packets to the SCADA master. The attacks are thus considered stealthy.

The detection accuracy and timing performance of the proposed anomaly detector are adequate for all the experiments with performance degradation (first scenario). That is, the results have 100% detection rates with false positive rates under 0.5%. In all of the experiments, our detector detects performance degradation before packet loss. With forged packets (second scenario), we found that our approach is effective for attacks in low-volume traffic and attacks lasting several hours. Compared to the time a targeted attack needs to pursue its objectives, a detector that sends alarms against attacks lasting several hours should be considered as efficient and effective.

Contributions. Using the datasets from a real power station, this paper shows that the spontaneous traffic contains stable and persistent attributes, namely limited group of inter-arrival times and correlation between flows. These two attributes are validated to be present in the dataset and do not change over phases in the data duration (one month). Since attacks are assumed to be absent in the normal (collected) traffic a particular challenge was to create realistic timing impacts of attacks. For this purpose, we implemented a simulator to generate testing datasets with attacks that have impact on time. The paper proposes an anomaly detection system combining the models based on these attributes. The results show that the proposed IDS is able to detect the first scenario with high accuracy and low FPR, whereas it can detect the second scenario only under certain conditions. This work demonstrates that network-based anomaly detection for spontaneous events is ambitious but possible and can be used as a foundation for future research in this area.

1.6 Conclusions and Future Work

To conclude, this research contributes to three main knowledge gaps regarding network-based anomaly detection for SCADA systems. First, a statistical approach that is able to detect subtle changes in timing is effective for request-response traffic such as Modbus traffic, but as far as we can see in our collected data sets, a large amount of IEC-104 SCADA traffic is generated by the non-requested communication mode. Second, this work adopts pattern mining techniques on IEC-104 non-requested traffic and discovers this traffic exhibits a certain level of timing regularity. That is, SCADA traffic in both request-response communication and spontaneous communication modes contains stable and persistent attributes. Third, this work demonstrates that a timing approach to network-based anomaly detection for non-requested traffic is ambitious but possible. Given the real-world data available to us, the modeling approaches for spontaneous traffic in non-requested communication mode are effective under most of the conditions.

The main challenge for anomaly-based intrusion detection system in SCADA networks is the lack of openly sharable datasets to compare different approaches. Due to the confidential nature of real data, most of the research work in this domain is tested and evaluated with emulated/simulated datasets collected from testbeds or non-open datasets collected from some real-world SCADA systems. Although some testbeds provide data with availability upon request [74], data sharing between researchers is still in its infancy. We need more openly available datasets with different attack scenarios and network settings to evaluate the proposed defense mechanisms for SCADA systems. One possible solution is to collect more datasets from real SCADA systems and conduct a comparative analysis between the real-world and synthetic datasets. The results of comparative analysis can be a basis for generating emulated data in the virtualized testbed [3] developed in our project, which is intended to be open for training and experiments. With the virtualized testbed people can study more attack scenarios and generate traffic with attacks for IDS benchmarking.

Another known challenge for anomaly-based intrusion detection systems in SCADA networks is the changes of the systems such as phase transitions caused by regular process workflows as observed in Paper B. In addition, a critical infrastructure facility may make changes such as reconfigurations to adapt to the current demand or supply status. The reconfiguration may cause sudden changes in the traffic which become the source of false positives. Currently, we try to choose the characteristics that are robust against phase transitions as proposed in Paper C and accept all the minor bursts and noises in the training traffic as normality without understanding it. With an understanding of the impact of reconfiguration and phase transitions, one might be able to make use of more features and network attributes with lower FPR. There are two possible ways to address the phase transition and the reconfiguration problem. The first option is to identify phase transitions and learn the normality model separately for each phase. If the operation log is available, we can also identify the reconfigurations and learn it as part of the normality. This type of IDSs require long training datasets and operation logs which are hard to access for research purposes. The second option is to develop adaptive intrusion detection systems that re-learn the model when they identify a phase transition. However, this type of IDS can be prone to poisoning attacks. Both of them are emerging research topics in the SCADA security domain.



Bibliography

- [1] Chuadhry Mujeeb Ahmed, Martin Ochoa, Jianying Zhou, Aditya P. Mathur, Rizwan Qadeer, Carlos Murguia, and Justin Ruths. “NoisePrint: Attack Detection Using Sensor and Process Noise Fingerprint in Cyber Physical Systems”. In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security (ASIACCS)*. ASIACCS ’18. ACM, 2018. DOI: 10.1145/3196494.3196532.
- [2] Chuadhry Mujeeb Ahmed, Jianying Zhou, and Aditya 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 (ACSAC)*. ACM, 2018, pp. 566–581. DOI: 10.1145/3274694.3274748.
- [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”. In: *Critical Information Infrastructures Security (CRITIS)*. LNCS, Springer, 2019.
- [4] sKyWIper Analysis Team. *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks*. Tech. rep. Laboratory of Cryptography, System Security (CrySyS Lab), Budapest University of Technology, and Economics Department of Telecommunications, 2012. URL: <https://www.crysys.hu/publications/files/skywiper.pdf>.
- [5] Oxana Andreeva, Sergey Gordeychik, Gleb Gritsai, Olga Kochetova, Evgeniya Potseluevskaya, Sergey I. Sidorov, and Alexander A. Timo-

- rin. *Industrial control systems vulnerabilities statistics*. Tech. rep. Kaspersky Lab, 2016. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190426/KL_REPORT_ICS_Statistic_vulnerabilities.pdf.
- [6] Simon Duque Anton, Lia Ahrens, Daniel Fraunholz, and Hans D. Schotten. “Time is of the Essence: Machine Learning-based Intrusion Detection in Industrial Time Series Data”. In: *Proceedings of International Conference on Data Mining Workshops (ICDMW)*. IEEE, 2018.
- [7] Wissam Aoudi, Mikel Iturbe, and Magnus Almgren. “Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems”. In: *Proceedings of the Conference on Computer and Communications Security*. ACM, 2018.
- [8] Abdullah Khalili and Ashkan Sami, Amin Khozaei, and Saber Poursmaeeli. “SIDS: State-based intrusion detection for stage-based cyber physical systems”. In: *International Journal of Critical Infrastructure Protection* (2018).
- [9] Rima Asmar Awad, Saeed Beztchi, Jared M Smith, Bryan Lyles, and Stacy Prowell. “Tools, Techniques, and Methodologies: A Survey of Digital Forensics for SCADA Systems”. In: *Proceedings of the 4th Annual Industrial Control System Security Workshop (ICSS)*. 2018.
- [10] Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras. “Difficulties in Modeling SCADA Traffic: A Comparative Analysis”. In: *Passive and Active Measurement. (PAM)*. LNCS, Springer, 2012.
- [11] Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras. “Exploiting Traffic Periodicity in Industrial Control Networks”. In: *International Journal of Critical Infrastructure Protection* 13 (2016), pp. 52–62.
- [12] Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras. “Flow whitelisting in SCADA networks”. In: *International Journal of Critical Infrastructure Protection* 6 (2013), pp. 150–158.
- [13] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Márk Félegyházi. *Duqu: A Stuxnet-like malware found in the wild*. Tech. rep. Laboratory of Cryptography, System Security (CrySyS Lab), Budapest University of Technology, and Economics Department of Telecommunications, 2011. URL: <https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf>.
- [14] Sajal Bhatia, Nishchal Kush, Chris Djameludin, Ayodeji Akande, and Ernest Foo. “Practical Modbus flooding attack and detection”. In: *Proceedings of Australasian Information Security Conference (ACSW-AISC)*. Australian Computer Society, Inc., 2014.

-
- [15] John Bigham, David Gamez, and Ning Lu. "Safeguarding SCADA Systems with Anomaly Detection". In: *Computer Network Security (MMM-ACNS)*. LNCS, Springer, 2003.
- [16] Alexander Borek, Ajith K.Parlikad, Jela Webb, and Philip Woodall. "Total Information Risk Management". In: Elsevier Inc., 2014. Chap. 4, pp. 47–56.
- [17] Eric Byres and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems". In: *Proceedings of the VDE Kongress*. VDE Association for Electrical Electronic & Information Technologies, 2004.
- [18] Andrea Carcano, Alessio Coletta, Michele Guglielmi, Marcelo Masera, Igor Nai Fovino, and Alberto Trombetta. "A multidimensional critical state analysis for detecting intrusions in SCADA systems". In: *IEEE Transactions on Industrial Informatics* (2011).
- [19] Andrea Carcano, Igor Nai Fovino, Marcelo Masera, and Alberto Trombetta. "State-Based Network Intrusion Detection Systems for SCADA Protocols: A Proof of Concept". In: *Critical Information Infrastructures Security (CRITIS)*. LNCS, Springer, 2009.
- [20] Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response". In: *Proceedings of the 6th Symposium on Information, Computer and Communications Security (ASIACCS)*. ACM, 2011.
- [21] Marco Caselli, Emmanuele Zambon, Johanna Amann, Robin Sommer, and Frank Kargl. "Specification Mining for Intrusion Detection in Networked Control Systems". In: *Proceedings of 25th USENIX Security Symposium (USENIX Security)*. USENIX Association, 2016.
- [22] Marco Caselli, Emmanuele Zambon, and Frank Kargl. "Sequence-aware Intrusion Detection in Industrial Control Systems." In: *Proceedings of the 1st Workshop on Cyber-Physical System Security (CPSS)*. ACM, 2015.
- [23] Marco Caselli, Emmanuele Zambon, Jonathan Petit, and Frank Kargl. "Modeling Message Sequences for Intrusion Detection in Industrial Control Systems". In: *Critical Infrastructure Protection IX (ICCIP)* (2015), pp. 49–71.
- [24] Raghavendra Chalapathy and Sanjay Chawla. "Deep Learning for Anomaly Detection: A Survey". In: *arXiv:1901.03407*. arXiv:1901.03407, 2019.

- [25] Binbin Chen, Xinshu Dong, Guangdong Bai, Sumeet Jauhar, and Yueqiang Cheng. "Secure and Efficient Software-based Attestation for Industrial Control Devices with ARM Processors". In: *Proceedings of the 33rd Annual Computer Security Applications Conferences (ACSAC)*. ACM, 2017.
- [26] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin-Jones, Hugh Soulsby, and KristanStoddart. "A review of cyber security risk assessment methods for SCADA systems". In: *Computers and Security* 56 (2016), pp. 1–27.
- [27] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. "Using model-based intrusion detection for SCADA networks". In: *Proceedings of the SCADA Security Scientific Symposium (S4)*. ISSSource, 2007.
- [28] J. J. Chromik, A. Remke, and B. R. Haverkort. "What's under the hood? Improving SCADA security with process awareness". In: *Proceedings of Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*. IEEE, 2016.
- [29] Gordon Clarke and Deon Reynders. *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*. Newnes, 2004.
- [30] *Distributed Network Protocol 3.0*. URL: <https://www.dnp.org/pages/aboutdefault.aspx>.
- [31] Patrick Düssel, Christian Gehl, Pavel Laskov, Jens-Uwe Bußer, Christof Störmann, and Jan Kästner. "Cyber-Critical Infrastructure Protection Using Real-Time Payload-Based Anomaly Detection". In: *Critical Information Infrastructures Security (CRITIS)*. LNCS, Springer, 2010.
- [32] Herson Esquivel-Vargas, Marco Caselli, and Andreas Peter. "Automatic Deployment of Specification-based Intrusion Detection in the BACnet Protocol". In: *Proceedings of Workshop on Cyber-Physical Systems Security and Privacy (CPS)*. ACM, 2017.
- [33] Mustafa Faisal, Alvaro A. Cardenas, and Avishai Wool. "Modeling Modbus TCP for intrusion detection". In: *Proceedings of Conference on Communications and Network Security (CNS)*. IEEE, 2016.
- [34] Nicolas Falliere, Liam O Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Tech. rep. Mountain View: Symantec, 2011.
- [35] Hamed Farsi, Ali Fanian, and Zahra Taghiyarrenani. "A novel online state-based anomaly detection system for process control networks". In: *International Journal of Critical Infrastructure Protection* (2019).

- [36] Cheng Feng, Tingting Li, and Deepthi Chana. "Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM networks". In: *Proceedings of the 47th Annual International Conference on Dependable Systems and Networks (DSN)*. IEEE/IFIP, 2017.
- [37] David Formby, Anwar Walid, and Rahhem Beyah. "A Case Study in Power Substation Network Dynamics". In: *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 1.19 (2017).
- [38] Igor Nai Fovino, Andrea Carcano, Thibault De Lacheze Murel, Alberto Trombetta, and Marcelo Masera. "Modbus/DNP3 state-based intrusion detection system". In: *Proceedings of the 24th International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2010.
- [39] Inaki Garitano, Christos Siaterlis, Bela Genge, Roberto Uribeetxeberria, and Urko Zurutuza. "A method to construct network traffic models for process control systems". In: *Proceedings of the 17th Conference on Emerging Technologies Factory Automation (ETFA)*. IEEE, 2012.
- [40] M. R. Gauthama Raman, Nivethitha Somu, and Aditya P. Mathur. "Anomaly Detection in Critical Infrastructure Using Probabilistic Neural Network". In: *Applications and Techniques in Information Security*. Springer, 2019, pp. 129–141.
- [41] Ashish Gehani and Gershon Kedem. "RheoStat: Real-Time Risk Management". In: *Recent Advances in Intrusion Detection (RAID)*. LNCS, Springer, 2004.
- [42] Hamid Reza Ghaeini, Matthew Chan, Raad Bahmani, Ferdinand Brassler, Luis Garcia, Jianying Zhou, Ahmad-Reza Sadeghi, Nils Ole Tippenhauer, and Saman Zonouz. "PAtt: Physics-based Attestation of Control Systems". In: *Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*. USENIX Association, 2019.
- [43] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. "A Survey of Physics-Based Attack Detection in Cyber-Physical Systems". In: *ACM Computing Surveys* (2018).
- [44] Niv Goldenberg and Avishai Wool. "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems". In: *International Journal of Critical Infrastructure Protection* 6.2 (2013), pp. 63–75.
- [45] Dina Hadžiosmanović, Lorenzo Simionato, Damiano Bolzoni, Emanuele Zamboni, and Sandro Etalle. "N-Gram against the Machine: On the Feasibility of the N-Gram Network Analysis for Binary Protocols". In: *Research in Attacks, Intrusions, and Defenses (RAID)*. LNCS, Springer, 2012.

- [46] Dina Hadžiosmanović, Robin Sommer, Emmanuele Zambon, and Pieter H.Hartel. "Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes". In: *Proceedings of the 30th Annual Computer Security Applications Conference*. 2014.
- [47] Stephen Hilt, Numaan Huq, Vladimir Kropotov, Robert McArdle, Cedric Pernet, and Roel Reyes. *Exposed and vulnerable critical infrastructure: water and energy industries*. Tech. rep. TrendMicro Inc., 2018. URL: https://documents.trendmicro.com/assets/white_papers/wp-exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.pdf.
- [48] Josh Homan, Sean McBride, and Rob Caldwell. *IRONGATE ICS Malware: Nothing to See Here...Masking Malicious Activity on SCADA Systems*. Tech. rep. FireEye, 2016. URL: https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html.
- [49] Yan Hu, An Yang, Hong Li, Yuyan Sun, and Limin Sun. "A survey of intrusion detection on industrial control systems". In: *International Journal of Distributed Sensor Networks* 14.8 (2018).
- [50] IEC 60870-5-104. URL: <https://webstore.iec.ch/publication/25035>.
- [51] Asif Iqbal, Mathias Ekstedt, and Hanan Alobaidli. "Digital Forensic Readiness in Critical Infrastructures: A Case of Substation Automation in the Power Sector". In: *Digital Forensics and Cyber Crime (ICDF2C)*. LNCS, Springer, 2017.
- [52] Xuan Jin, John Bigham, Julian Rodaway, David Gamez, and Chris Phillips. "Anomaly Detection in Electricity Cyber Infrastructure". In: *Proceedings of International Workshop on Complex Networks and Infrastructure Protection (CNIP)*. 2006.
- [53] Khurum Nazir Junejo and Jonathan Goh. "Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning". In: *Proceedings of the 2nd International Workshop on Cyber-Physical System Security*. ACM, 2016.
- [54] Boudewijn R. Haverkort Justyna J. Chromik Anne Remke. "Improving SCADA security of a local process with a power grid model". In: *Proceedings of 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*. 2016.
- [55] István Kiss, Béla Genge, and Piroska Haller. "A clustering-based approach to detect cyber attacks in process control systems". In: *Proceedings of the 13th International Conference on Industrial Informatics (INDIN)*. IEEE, 2015.

- [56] Amit Kleinmann and Avishai Wool. "A Statechart-Based Anomaly Detection Model for Multi-Threaded SCADA Systems." In: *Critical Information Infrastructures Security (CRITIS)*. LNCS, Springer, 2016.
- [57] Amit Kleinmann and Avishai Wool. "Accurate Modeling of the Siemens S7 SCADA Protocol for Intrusion Detection and Digital Forensic". In: *The Journal of Digital Forensics, Security and Law* 9.2 (2014).
- [58] Amit Kleinmann and Avishai Wool. "Automatic Construction of Statechart-Based Anomaly Detection Models for Multi-Threaded SCADA via Spectral Analysis". In: *Proceedings of the 2nd Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*. ACM, 2016.
- [59] Christian Kreibich and Jon Crowcroft. "Honeycomb: creating intrusion detection signatures using honeypots". In: *Proceedings of the 2nd Workshop on Hot Topics in Networks*. ACM SIGCOMM, 2004.
- [60] Marina Krotofil, Jason Larson, and Dieter Gollmann. "The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems." In: *Proceedings of the 10th Symposium on Information, Computer and Communications Security (ASIACCS)*. ACM, 2015.
- [61] David Kuipers and Mark Fabro. *Control Systems Cyber Security: Defense in Depth Strategies*. Tech. rep. U. S. Department of Energy National Laboratory, 2006.
- [62] Robert M. Lee, Michael J. Assante, and Tim Conway. *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. Tech. rep. Electricity Information Sharing and Analysis Center, 2016. URL: [https://ics.sans.org/media/\\$E-ISAC_SANS_Ukraine_DUC_5\\$.pdf](https://ics.sans.org/media/$E-ISAC_SANS_Ukraine_DUC_5$.pdf).
- [63] Chih-Yuan Lin and Simin Nadjm-Tehrani. "Timing Patterns and Correlations in Spontaneous SCADA Traffic for Anomaly Detection". In: *Proceedings of 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*. USENIX Association, 2019.
- [64] Chih-Yuan Lin and Simin Nadjm-Tehrani. "Understanding IEC-60870-5-104 Traffic Patterns in SCADA Networks". In: *Proceedings of the 4th Cyber-Physical System Security Workshop*. ACM, 2018.
- [65] Chih-Yuan Lin, Simin Nadjm-Tehrani, and Mikael Asplund. "Timing-based Anomaly Detection in SCADA networks". In: *Critical Information Infrastructures Security (CRITIS)*. Vol. 10707. LNCS, Springer, 2017. DOI: 10.1007/978-3-319-99843-5_5.
- [66] Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K. Iyer. "Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol". In: *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW)*. ACM, 2013.

- [67] Ondrej Linda, Milos Manic, Jim Alves-Foss, and Todd Vollmer. "Towards resilient critical infrastructures: Application of Type-2 Fuzzy Logic in embedded network security cyber sensor". In: *Proceedings of 4th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 2011.
- [68] Ondrej Linda, Milos Manic, and Todd Vollmer. "Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge". In: *Proceedings of the 5th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 2012.
- [69] Ondrej Linda, Milos Manic, Todd Vollmer, and Jason Wright. "Fuzzy logic based anomaly detection for embedded network security cyber sensor". In: *Proceedings of Symposium on Computational Intelligence in Cyber Security (CICS)*. IEEE, 2011.
- [70] Ondrej Linda, Todd Vollmer, and Milos Manic. "Neural Network based Intrusion Detection System for critical infrastructures". In: *Proceedings of International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2009.
- [71] Leandros A. Maglaras and Jianmin Jiang. "Intrusion Detection in SCADA systems using Machine Learning Techniques". In: *Proceedings of Science and Information Conference (SAI)*. IEEE, 2014.
- [72] Chen Markman, Avishai Wool, and Alvaro A. Cardenas. "A New Burst-DFA model for SCADA Anomaly Detection". In: *Proceedings of Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*. ACM, 2017.
- [73] Chen Markman, Avishai Wool, and Alvaro A. Cardenas. "Temporal Phase Shifts in SCADA Networks". In: *Proceedings of Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*. ACM, 2018.
- [74] Aditya P. Mathur and Nils Ole Tippenhauer. "SWaT: a water treatment testbed for research and training on ICS security". In: *Proceedings of International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. IEEE, 2016.
- [75] Stephen McLaughlin, Saman Zonouz, Devin Pohly, and Patrick McDaniel. "A Trusted Safety Verifier for Process Controller Code". In: *Proceedings of Network and Distributed System Security Symposium (NDSS)*. 2014.
- [76] Robert Mitchell and Ing-Ray Chen. "A survey of intrusion detection techniques for cyber-physical systems". In: *ACM Computing Surveys* (2014).
- [77] Robert Mitchell and Ing-Ray Chen. "Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications". In: *IEEE Transactions on Smart Grid* (2013).

- [78] *Modbus*. URL: <http://www.modbus.org/>.
- [79] Steve Muller. "Risk monitoring with intrusion detection for industrial control systems". PhD thesis. Ecole nationale supérieure Mines-Télécom Atlantique, 2018.
- [80] Patric Nader, Paul Honeine, and Pierre Beuseroy. "Lp-Norms in One-Class Classification for Intrusion Detection in SCADA Systems". In: *IEEE Transactions on Industrial Informatics* (2014).
- [81] Jeyasingam Nivethan and Mauricio Papa. "Dynamic rule generation for SCADA intrusion detection". In: *Proceedings of Symposium on Technologies for Homeland Security (HST)*. IEEE, 2016.
- [82] Shengyi Pan, Thomas Morris, and Uttam Adhikari. "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems". In: *IEEE Transactions on Smart Grid* (2015).
- [83] Masood Parvania, Georgia Koutsandria, Vishak Muthukumary, Sean Peisert, Chuck McParland, and Anna Scaglione. "Hybrid Control Network Intrusion Detection Systems for Automated Power Distribution Systems". In: *Proceedings of the 44th Annual International Conference on Dependable Systems and Networks*. IEEE/IFIP, 2014.
- [84] Adrian Pauna, Konstantinos Moulinos, Matina Lakka, John May, and Theo Tryfonas. *Can we learn from SCADA security incidents?* Tech. rep. European Union Agency for Cybersecurity, 2003.
- [85] Naoum Sayegh, Imad H. Elhaji, Ayman Kayssi, and Ali Chehab. "SCADA Intrusion Detection System Based on Temporal Behavior of Frequent Patterns." In: *Proceedings of 17th Mediterranean Electrotechnical Conference (MELECON)*. IEEE, 2014.
- [86] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. "PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks". In: *Proceedings of the 22nd Conference on Computer and Communications Security*. ACM SIGSAC, 2015.
- [87] International Organization for Standardization. *ISO/IEC 27005: information security risk management*. 2008.
- [88] Industrial Control Systems Cyber Emergency Response Team. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. Tech. rep. U. S. Department of Homeland Security, 2016.
- [89] Robert Udd, Mikael Asplund, Simin Nadjm-Tehrani, Mehrdad Kazemtabrizi, and Mathias Ekstedt. "Exploiting Bro for Intrusion Detection in a SCADA System." In: *Proceedings of the 2nd International Workshop on Cyber-Physical System Security (CPSS)*. ACM, 2016.

- [90] Alfonso Valdes and Steven Cheung. "Communication pattern anomaly detection in process control systems". In: *Proceedings of international Conference on Technologies for Homeland Security*. IEEE, 2009.
- [91] Craig Valli. "SCADA Forensics with Snort IDS". In: *Proceedings of the International Conference Security and Management (SAM)*. CSREA Press, 2009, pp. 618–621.
- [92] Emmanouil Vasilomanolakis, Shreyas Srinivasa, Carlos Garcia Cordero, and Max Muhlhäuser. "Multi-stage Attack Detection and Signature Generation with ICS Honeypots". In: *Proceedings of Workshop on Security for Emerging Distributed Network Technologies (DISSECT)*. IEEE/IFIP, 2016.
- [93] Pin-Han Wang, I-En Liao, Kuo-Fong Kao, and Jyun-Yao Huang. "An intrusion detection method based on log sequence clustering of honeypot for Modbus TCP protocol". In: *Proceedings of International Conference on Applied System Invention (ICASI)*. IEEE, 2018.
- [94] Kevin Wong, Craig Dillabaugh, Nabil Seddigh, and Biswajit Nandy. "Enhancing Suricata intrusion detection system for cyber security in SCADA networks". In: *Proceedings of the 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 2017.
- [95] Christian Wressnegger, Ansgar Kellner, and Konrad Rieck. "ZOE: Content-Based Anomaly Detection for Industrial Control Systems". In: *Proceedings of 48th Annual International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2018.
- [96] Yu-jun Xiao, Wen-yuan Xu, Zhen-hua Jia, Zhuo-ran Ma, and Dong-lian Qi. "NIPAD: A Non-Invasive Power-Based Anomaly Detection Scheme for Programmable Logic Controllers". In: *Frontiers of Information Technology & Electronic Engineering* (2017).
- [97] Y. Yang, K. McLaughlin, S. Sezer, Y.B. Yuan, and W. Huang. "Stateful intrusion detection for IEC-60870-5-104 SCADA security". In: *Proceedings of PES General Meeting*. IEEE, 2014.
- [98] Yi Yang, kieran Mclaughlin, Tim Littler, Sakir Sezer, and H. F. Wang. "Rule-based intrusion detection system for SCADA networks". In: *Proceedings of the 2nd IET Renewable Power Generation Conference (RPG)*. 2013.
- [99] Man-Ki Yoon and Gabriela Ciocarlie. "Communication Pattern Monitoring: Improving the Utility of Anomaly Detection for Industrial Control Systems". In: *Proceedings of Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2014.

Papers

The papers associated with this thesis have been removed for copyright reasons. For more details about these see:

<http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-165155>

Department of Computer and Information Science
Linköpings universitet

Licentiate Theses

Linköpings Studies in Science and Technology
Faculty of Arts and Sciences

- No 17 **Vojin Plavsic:** Interleaved Processing of Non-Numerical Data Stored on a Cyclic Memory. (Available at: FOA, Box 1165, S-581 11 Linköping, Sweden. FOA Report B30062E)
- No 28 **Arne Jönsson, Mikael Patel:** An Interactive Flowcharting Technique for Communicating and Realizing Algorithms, 1984.
- No 29 **Johnny Eckerland:** Retargeting of an Incremental Code Generator, 1984.
- No 48 **Henrik Nordin:** On the Use of Typical Cases for Knowledge-Based Consultation and Teaching, 1985.
- No 52 **Zebo Peng:** Steps Towards the Formalization of Designing VLSI Systems, 1985.
- No 60 **Johan Fagerström:** Simulation and Evaluation of Architecture based on Asynchronous Processes, 1985.
- No 71 **Jalal Maleki:** ICONStraint, A Dependency Directed Constraint Maintenance System, 1987.
- No 72 **Tony Larsson:** On the Specification and Verification of VLSI Systems, 1986.
- No 73 **Ola Strömfors:** A Structure Editor for Documents and Programs, 1986.
- No 74 **Christos Levcopoulos:** New Results about the Approximation Behavior of the Greedy Triangulation, 1986.
- No 104 **Shamsul I. Chowdhury:** Statistical Expert Systems - a Special Application Area for Knowledge-Based Computer Methodology, 1987.
- No 108 **Rober Bilos:** Incremental Scanning and Token-Based Editing, 1987.
- No 111 **Hans Block:** SPORT-SORT Sorting Algorithms and Sport Tournaments, 1987.
- No 113 **Ralph Rönquist:** Network and Lattice Based Approaches to the Representation of Knowledge, 1987.
- No 118 **Mariam Kamkar, Nahid Shahmehri:** Affect-Chaining in Program Flow Analysis Applied to Queries of Programs, 1987.
- No 126 **Dan Strömberg:** Transfer and Distribution of Application Programs, 1987.
- No 127 **Kristian Sandahl:** Case Studies in Knowledge Acquisition, Migration and User Acceptance of Expert Systems, 1987.
- No 139 **Christer Bäckström:** Reasoning about Interdependent Actions, 1988.
- No 140 **Mats Wirén:** On Control Strategies and Incrementality in Unification-Based Chart Parsing, 1988.
- No 146 **Johan Hultman:** A Software System for Defining and Controlling Actions in a Mechanical System, 1988.
- No 150 **Tim Hansen:** Diagnosing Faults using Knowledge about Malfunctioning Behavior, 1988.
- No 165 **Jonas Löwgren:** Supporting Design and Management of Expert System User Interfaces, 1989.
- No 166 **Ola Petersson:** On Adaptive Sorting in Sequential and Parallel Models, 1989.
- No 174 **Yngve Larsson:** Dynamic Configuration in a Distributed Environment, 1989.
- No 177 **Peter Åberg:** Design of a Multiple View Presentation and Interaction Manager, 1989.
- No 181 **Henrik Eriksson:** A Study in Domain-Oriented Tool Support for Knowledge Acquisition, 1989.
- No 184 **Ivan Rankin:** The Deep Generation of Text in Expert Critiquing Systems, 1989.
- No 187 **Simin Nadjm-Tehrani:** Contributions to the Declarative Approach to Debugging Prolog Programs, 1989.
- No 189 **Magnus Merkel:** Temporal Information in Natural Language, 1989.
- No 196 **Ulf Nilsson:** A Systematic Approach to Abstract Interpretation of Logic Programs, 1989.
- No 197 **Staffan Bonnier:** Horn Clause Logic with External Procedures: Towards a Theoretical Framework, 1989.
- No 203 **Christer Hansson:** A Prototype System for Logical Reasoning about Time and Action, 1990.
- No 212 **Björn Fjellborg:** An Approach to Extraction of Pipeline Structures for VLSI High-Level Synthesis, 1990.
- No 230 **Patrick Doherty:** A Three-Valued Approach to Non-Monotonic Reasoning, 1990.
- No 237 **Tomas Sokolnicki:** Coaching Partial Plans: An Approach to Knowledge-Based Tutoring, 1990.
- No 250 **Lars Strömberg:** Postmortem Debugging of Distributed Systems, 1990.
- No 253 **Torbjörn Näslund:** SL DFA-Resolution - Computing Answers for Negative Queries, 1990.
- No 260 **Peter D. Holmes:** Using Connectivity Graphs to Support Map-Related Reasoning, 1991.
- No 283 **Olof Johansson:** Improving Implementation of Graphical User Interfaces for Object-Oriented Knowledge- Bases, 1991.
- No 298 **Rolf G Larsson:** Aktivitetsbaserad kalkylering i ett nytt ekonomisystem, 1991.
- No 318 **Lena Srömbäck:** Studies in Extended Unification-Based Formalism for Linguistic Description: An Algorithm for Feature Structures with Disjunction and a Proposal for Flexible Systems, 1992.
- No 319 **Mikael Petterson:** DML-A Language and System for the Generation of Efficient Compilers from Denotational Specification, 1992.
- No 326 **Andreas Kägedal:** Logic Programming with External Procedures: an Implementation, 1992.
- No 328 **Patrick Lambrix:** Aspects of Version Management of Composite Objects, 1992.
- No 333 **Xinli Gu:** Testability Analysis and Improvement in High-Level Synthesis Systems, 1992.
- No 335 **Torbjörn Näslund:** On the Role of Evaluations in Iterative Development of Managerial Support Systems, 1992.
- No 348 **Ulf Cederling:** Industrial Software Development - a Case Study, 1992.
- No 352 **Magnus Morin:** Predictable Cyclic Computations in Autonomous Systems: A Computational Model and Implementation, 1992.
- No 371 **Mehran Noghabai:** Evaluation of Strategic Investments in Information Technology, 1993.
- No 378 **Mats Larsson:** A Transformational Approach to Formal Digital System Design, 1993.

- No 380 **Johan Ringström:** Compiler Generation for Parallel Languages from Denotational Specifications, 1993.
- No 381 **Michael Jansson:** Propagation of Change in an Intelligent Information System, 1993.
- No 383 **Jonni Harrius:** An Architecture and a Knowledge Representation Model for Expert Critiquing Systems, 1993.
- No 386 **Per Österling:** Symbolic Modelling of the Dynamic Environments of Autonomous Agents, 1993.
- No 398 **Johan Boye:** Dependency-based Groudnness Analysis of Functional Logic Programs, 1993.
- No 402 **Lars Degerstedt:** Tabulated Resolution for Well Founded Semantics, 1993.
- No 406 **Anna Moborg:** Satellitkontor - en studie av kommunikationsmönster vid arbete på distans, 1993.
- No 414 **Peter Carlsson:** Separation av företagsledning och finansiering - fallstudier av företagsledarutköp ur ett agent-teoretiskt perspektiv, 1994.
- No 417 **Camilla Sjöström:** Revision och lagreglering - ett historiskt perspektiv, 1994.
- No 436 **Cecilia Sjöberg:** Voices in Design: Argumentation in Participatory Development, 1994.
- No 437 **Lars Viklund:** Contributions to a High-level Programming Environment for a Scientific Computing, 1994.
- No 440 **Peter Loborg:** Error Recovery Support in Manufacturing Control Systems, 1994.
- FHS 3/94 **Owen Eriksson:** Informationssystem med verksamhetskvalitet - utvärdering baserat på ett verksamhetsinriktat och samskapande perspektiv, 1994.
- FHS 4/94 **Karin Pettersson:** Informationssystemstrukturering, ansvarsfördelning och användarinflytande - En komparativ studie med utgångspunkt i två informationssystemstrategier, 1994.
- No 441 **Lars Poignant:** Informationsteknologi och företagsetablering - Effekter på produktivitet och region, 1994.
- No 446 **Gustav Fahl:** Object Views of Relational Data in Multidatabase Systems, 1994.
- No 450 **Henrik Nilsson:** A Declarative Approach to Debugging for Lazy Functional Languages, 1994.
- No 451 **Jonas Lind:** Creditor - Firm Relations: an Interdisciplinary Analysis, 1994.
- No 452 **Martin Sköld:** Active Rules based on Object Relational Queries - Efficient Change Monitoring Techniques, 1994.
- No 455 **Pär Carlshamre:** A Collaborative Approach to Usability Engineering: Technical Communicators and System Developers in Usability-Oriented Systems Development, 1994.
- FHS 5/94 **Stefan Cronholm:** Varför CASE-verktyg i systemutveckling? - En motiv- och konsekvensstudie avseende arbetssätt och arbetsformer, 1994.
- No 462 **Mikael Lindvall:** A Study of Traceability in Object-Oriented Systems Development, 1994.
- No 463 **Fredrik Nilsson:** Strategi och ekonomisk styrning - En studie av Sandviks förvärv av Bahco Verktyg, 1994.
- No 464 **Hans Olén:** Collage Induction: Proving Properties of Logic Programs by Program Synthesis, 1994.
- No 469 **Lars Karlsson:** Specification and Synthesis of Plans Using the Features and Fluents Framework, 1995.
- No 473 **Ulf Söderman:** On Conceptual Modelling of Mode Switching Systems, 1995.
- No 475 **Choong-ho Yi:** Reasoning about Concurrent Actions in the Trajectory Semantics, 1995.
- No 476 **Bo Lagerström:** Successiv resultatavräkning av pågående arbeten. - Fallstudier i tre byggföretag, 1995.
- No 478 **Peter Jonsson:** Complexity of State-Variable Planning under Structural Restrictions, 1995.
- FHS 7/95 **Anders Avdic:** Arbetsintegrerad systemutveckling med kalkylprogram, 1995.
- No 482 **Eva L Ragnemalm:** Towards Student Modelling through Collaborative Dialogue with a Learning Companion, 1995.
- No 488 **Eva Toller:** Contributions to Parallel Multiparadigm Languages: Combining Object-Oriented and Rule-Based Programming, 1995.
- No 489 **Erik Stoy:** A Petri Net Based Unified Representation for Hardware/Software Co-Design, 1995.
- No 497 **Johan Herber:** Environment Support for Building Structured Mathematical Models, 1995.
- No 498 **Stefan Svenberg:** Structure-Driven Derivation of Inter-Lingual Functor-Argument Trees for Multi-Lingual Generation, 1995.
- No 503 **Hee-Cheol Kim:** Prediction and Postdiction under Uncertainty, 1995.
- FHS 8/95 **Dan Fristedt:** Metoder i användning - mot förbättring av systemutveckling genom situationell metodkunskap och metodanalys, 1995.
- FHS 9/95 **Malin Bergvall:** Systemförvaltning i praktiken - en kvalitativ studie avseende centrala begrepp, aktiviteter och ansvarsroller, 1995.
- No 513 **Joachim Karlsson:** Towards a Strategy for Software Requirements Selection, 1995.
- No 517 **Jakob Axelsson:** Schedulability-Driven Partitioning of Heterogeneous Real-Time Systems, 1995.
- No 518 **Göran Forslund:** Toward Cooperative Advice-Giving Systems: The Expert Systems Experience, 1995.
- No 522 **Jörgen Andersson:** Bilder av småföretagares ekonomistyrning, 1995.
- No 538 **Staffan Flodin:** Efficient Management of Object-Oriented Queries with Late Binding, 1996.
- No 545 **Vadim Engelson:** An Approach to Automatic Construction of Graphical User Interfaces for Applications in Scientific Computing, 1996.
- No 546 **Magnus Werner :** Multidatabase Integration using Polymorphic Queries and Views, 1996.
- FiF-a 1/96 **Mikael Lind:** Affärsprocessinriktad förändringsanalys - utveckling och tillämpning av synsätt och metod, 1996.
- No 549 **Jonas Hallberg:** High-Level Synthesis under Local Timing Constraints, 1996.
- No 550 **Kristina Larsen:** Förutsättningar och begränsningar för arbete på distans - erfarenheter från fyra svenska företag. 1996.
- No 557 **Mikael Johansson:** Quality Functions for Requirements Engineering Methods, 1996.
- No 558 **Patrik Nordling:** The Simulation of Rolling Bearing Dynamics on Parallel Computers, 1996.
- No 561 **Anders Ekman:** Exploration of Polygonal Environments, 1996.
- No 563 **Niclas Andersson:** Compilation of Mathematical Models to Parallel Code, 1996.

- No 567 **Johan Jenvald:** Simulation and Data Collection in Battle Training, 1996.
- No 575 **Niclas Ohlsson:** Software Quality Engineering by Early Identification of Fault-Prone Modules, 1996.
- No 576 **Mikael Ericsson:** Commenting Systems as Design Support—A Wizard-of-Oz Study, 1996.
- No 587 **Jörgen Lindström:** Chefers användning av kommunikationsteknik, 1996.
- No 589 **Esa Falkenroth:** Data Management in Control Applications - A Proposal Based on Active Database Systems, 1996.
- No 591 **Niclas Wahllöf:** A Default Extension to Description Logics and its Applications, 1996.
- No 595 **Annika Larsson:** Ekonomisk Styrning och Organisatorisk Passion - ett interaktivt perspektiv, 1997.
- No 597 **Ling Lin:** A Value-based Indexing Technique for Time Sequences, 1997.
- No 598 **Rego Granlund:** C³Fire - A Microworld Supporting Emergency Management Training, 1997.
- No 599 **Peter Ingels:** A Robust Text Processing Technique Applied to Lexical Error Recovery, 1997.
- No 607 **Per-Arne Persson:** Toward a Grounded Theory for Support of Command and Control in Military Coalitions, 1997.
- No 609 **Jonas S Karlsson:** A Scalable Data Structure for a Parallel Data Server, 1997.
- FiF-a 4 **Carita Åbom:** Videomötesteknik i olika affärsituationer - möjligheter och hinder, 1997.
- FiF-a 6 **Tommy Wedlund:** Att skapa en företagsanpassad systemutvecklingsmodell - genom rekonstruktion, värdering och vidareutveckling i T50-bolag inom ABB, 1997.
- No 615 **Silvia Coradeschi:** A Decision-Mechanism for Reactive and Coordinated Agents, 1997.
- No 623 **Jan Ollinen:** Det flexibla kontorets utveckling på Digital - Ett stöd för multiflex? 1997.
- No 626 **David Byers:** Towards Estimating Software Testability Using Static Analysis, 1997.
- No 627 **Fredrik Eklund:** Declarative Error Diagnosis of GAPLog Programs, 1997.
- No 629 **Gunilla Ivelfors:** Krigsspel och Informationsteknik inför en oförutsägbart framtid, 1997.
- No 631 **Jens-Olof Lindh:** Analysing Traffic Safety from a Case-Based Reasoning Perspective, 1997
- No 639 **Jukka Mäki-Turja:** Smalltalk - a suitable Real-Time Language, 1997.
- No 640 **Juha Takkinen:** CAFE: Towards a Conceptual Model for Information Management in Electronic Mail, 1997.
- No 643 **Man Lin:** Formal Analysis of Reactive Rule-based Programs, 1997.
- No 653 **Mats Gustafsson:** Bringing Role-Based Access Control to Distributed Systems, 1997.
- FiF-a 13 **Boris Karlsson:** Metodanalys för förståelse och utveckling av systemutvecklingsverksamhet. Analys och värdering av systemutvecklingsmodeller och dess användning, 1997.
- No 674 **Marcus Bjärelund:** Two Aspects of Automating Logics of Action and Change - Regression and Tractability, 1998.
- No 676 **Jan Håkegård:** Hierarchical Test Architecture and Board-Level Test Controller Synthesis, 1998.
- No 668 **Per-Ove Zetterlund:** Normering av svensk redovisning - En studie av tillkomsten av Redovisningsrådets rekommendation om koncernredovisning (RR01:91), 1998.
- No 675 **Jimmy Tjäder:** Projektledaren & planen - en studie av projektledning i tre installations- och systemutvecklingsprojekt, 1998.
- FiF-a 14 **Ulf Melin:** Informationssystem vid ökad affärs- och processorientering - egenskaper, strategier och utveckling, 1998.
- No 695 **Tim Heyer:** COMPASS: Introduction of Formal Methods in Code Development and Inspection, 1998.
- No 700 **Patrik Hägglund:** Programming Languages for Computer Algebra, 1998.
- FiF-a 16 **Marie-Therese Christiansson:** Inter-organisatorisk verksamhetsutveckling - metoder som stöd vid utveckling av partnerskap och informationssystem, 1998.
- No 712 **Christina Wennestam:** Information om immateriella resurser. Investeringar i forskning och utveckling samt i personal inom skogsindustrin, 1998.
- No 719 **Joakim Gustafsson:** Extending Temporal Action Logic for Ramification and Concurrency, 1998.
- No 723 **Henrik André-Jönsson:** Indexing time-series data using text indexing methods, 1999.
- No 725 **Erik Larsson:** High-Level Testability Analysis and Enhancement Techniques, 1998.
- No 730 **Carl-Johan Westin:** Informationsförsörjning: en fråga om ansvar - aktiviteter och uppdrag i fem stora svenska organisationers operativa informationsförsörjning, 1998.
- No 731 **Åse Jansson:** Miljöhänsyn - en del i företags styrning, 1998.
- No 733 **Thomas Padron-McCarthy:** Performance-Polymorphic Declarative Queries, 1998.
- No 734 **Anders Bäckström:** Värdeskapande kreditgivning - Kreditriskhantering ur ett agentteoretiskt perspektiv, 1998.
- FiF-a 21 **Ulf Seigerroth:** Integration av förändringsmetoder - en modell för välgrundad metodintegration, 1999.
- FiF-a 22 **Fredrik Öberg:** Object-Oriented Frameworks - A New Strategy for Case Tool Development, 1998.
- No 737 **Jonas Mellin:** Predictable Event Monitoring, 1998.
- No 738 **Joakim Eriksson:** Specifying and Managing Rules in an Active Real-Time Database System, 1998.
- FiF-a 25 **Bengt E W Andersson:** Samverkande informationssystem mellan aktörer i offentliga åtaganden - En teori om aktörsarenor i samverkan om utbyte av information, 1998.
- No 742 **Pawel Pietrzak:** Static Incorrectness Diagnosis of CLP (FD), 1999.
- No 748 **Tobias Ritzau:** Real-Time Reference Counting in RT-Java, 1999.
- No 751 **Anders Ferntoft:** Elektronisk affärskommunikation - kontaktkostnader och kontaktprocesser mellan kunder och leverantörer på producentmarknader, 1999.
- No 752 **Jo Skåmedal:** Arbete på distans och arbetsformens påverkan på resor och resmönster, 1999.
- No 753 **Johan Alvehus:** Mötets metaforer. En studie av berättelser om möten, 1999.

- No 754 **Magnus Lindahl:** Bankens villkor i låneavtal vid kreditgivning till högt belånade företagsförvärv: En studie ur ett agentteoretiskt perspektiv, 2000.
- No 766 **Martin V. Howard:** Designing dynamic visualizations of temporal data, 1999.
- No 769 **Jesper Andersson:** Towards Reactive Software Architectures, 1999.
- No 775 **Anders Henriksson:** Unique kernel diagnosis, 1999.
- FiF-a 30 **Pär J. Ågerfalk:** Pragmatization of Information Systems - A Theoretical and Methodological Outline, 1999.
- No 787 **Charlotte Björkegren:** Learning for the next project - Bearers and barriers in knowledge transfer within an organisation, 1999.
- No 788 **Håkan Nilsson:** Informationsteknik som drivkraft i granskningsprocessen - En studie av fyra revisionsbyråer, 2000.
- No 790 **Erik Berglund:** Use-Oriented Documentation in Software Development, 1999.
- No 791 **Klas Gäre:** Verksamhetsförändringar i samband med IS-införande, 1999.
- No 800 **Anders Subotic:** Software Quality Inspection, 1999.
- No 807 **Svein Bergum:** Managerial communication in telework, 2000.
- No 809 **Flavius Gruian:** Energy-Aware Design of Digital Systems, 2000.
- FiF-a 32 **Karin Hedström:** Kunskapsanvändning och kunskapsutveckling hos verksamhetskonsulter - Erfarenheter från ett FOU-samarbete, 2000.
- No 808 **Linda Askenäs:** Affärssystemet - En studie om teknikens aktiva och passiva roll i en organisation, 2000.
- No 820 **Jean Paul Meynard:** Control of industrial robots through high-level task programming, 2000.
- No 823 **Lars Hult:** Publika Gränssytor - ett designexempel, 2000.
- No 832 **Paul Pop:** Scheduling and Communication Synthesis for Distributed Real-Time Systems, 2000.
- FiF-a 34 **Göran Hultgren:** Nätverksinriktad Förändringsanalys - perspektiv och metoder som stöd för förståelse och utveckling av affärsrelationer och informationssystem, 2000.
- No 842 **Magnus Kald:** The role of management control systems in strategic business units, 2000.
- No 844 **Mikael Cäker:** Vad kostar kunden? Modeller för intern redovisning, 2000.
- FiF-a 37 **Ewa Braf:** Organisationers kunskapsverksamheter - en kritisk studie av "knowledge management", 2000.
- FiF-a 40 **Henrik Lindberg:** Webaserade affärsprocesser - Möjligheter och begränsningar, 2000.
- FiF-a 41 **Benneth Christiansson:** Att komponentbasera informationssystem - Vad säger teori och praktik?, 2000.
- No. 854 **Ola Pettersson:** Deliberation in a Mobile Robot, 2000.
- No 863 **Dan Lawesson:** Towards Behavioral Model Fault Isolation for Object Oriented Control Systems, 2000.
- No 881 **Johan Moe:** Execution Tracing of Large Distributed Systems, 2001.
- No 882 **Yuxiao Zhao:** XML-based Frameworks for Internet Commerce and an Implementation of B2B e-procurement, 2001.
- No 890 **Annika Flycht-Eriksson:** Domain Knowledge Management in Information-providing Dialogue systems, 2001.
- FiF-a 47 **Per-Arne Segerkvist:** Webaserade imaginära organisationers samverkansformer: Informationssystemarkitektur och aktörssamverkan som förutsättningar för affärsprocesser, 2001.
- No 894 **Stefan Svarén:** Styrning av investeringar i divisionaliserade företag - Ett koncernperspektiv, 2001.
- No 906 **Lin Han:** Secure and Scalable E-Service Software Delivery, 2001.
- No 917 **Emma Hansson:** Optionsprogram för anställda - en studie av svenska börsföretag, 2001.
- No 916 **Susanne Odar:** IT som stöd för strategiska beslut, en studie av datorimplementerade modeller av verksamhet som stöd för beslut om anskaffning av JAS 1982, 2002.
- FiF-a-49 **Stefan Holgersson:** IT-system och filtrering av verksamhetskunskap - kvalitetsproblem vid analyser och beslutsfattande som bygger på uppgifter hämtade från polisens IT-system, 2001.
- FiF-a-51 **Per Oscarsson:** Informationssäkerhet i verksamheter - begrepp och modeller som stöd för förståelse av informationssäkerhet och dess hantering, 2001.
- No 919 **Luis Alejandro Cortes:** A Petri Net Based Modeling and Verification Technique for Real-Time Embedded Systems, 2001.
- No 915 **Niklas Sandell:** Redovisning i skuggan av en bankkris - Värdering av fastigheter. 2001.
- No 931 **Fredrik Elg:** Ett dynamiskt perspektiv på individuella skillnader av heuristisk kompetens, intelligens, mentala modeller, mål och konfidens i kontroll av mikrovärlden Moro, 2002.
- No 933 **Peter Aronsson:** Automatic Parallelization of Simulation Code from Equation Based Simulation Languages, 2002.
- No 938 **Bourhane Kadmiry:** Fuzzy Control of Unmanned Helicopter, 2002.
- No 942 **Patrik Haslum:** Prediction as a Knowledge Representation Problem: A Case Study in Model Design, 2002.
- No 956 **Robert Sevenius:** On the instruments of governance - A law & economics study of capital instruments in limited liability companies, 2002.
- FiF-a 58 **Johan Petersson:** Lokala elektroniska marknadsplatser - informationssystem för platsbundna affärer, 2002.
- No 964 **Peter Bunus:** Debugging and Structural Analysis of Declarative Equation-Based Languages, 2002.
- No 973 **Gert Jervan:** High-Level Test Generation and Built-In Self-Test Techniques for Digital Systems, 2002.
- No 958 **Fredrika Berglund:** Management Control and Strategy - a Case Study of Pharmaceutical Drug Development, 2002.
- FiF-a 61 **Fredrik Karlsson:** Meta-Method for Method Configuration - A Rational Unified Process Case, 2002.
- No 985 **Sorin Manolache:** Schedulability Analysis of Real-Time Systems with Stochastic Task Execution Times, 2002.
- No 982 **Diana Szentiványi:** Performance and Availability Trade-offs in Fault-Tolerant Middleware, 2002.
- No 989 **Iakov Nakhimovski:** Modeling and Simulation of Contacting Flexible Bodies in Multibody Systems, 2002.
- No 990 **Levon Saldamli:** PDEModelica - Towards a High-Level Language for Modeling with Partial Differential Equations, 2002.
- No 991 **Almut Herzog:** Secure Execution Environment for Java Electronic Services, 2002.

- No 999 **Jon Edvardsson:** Contributions to Program- and Specification-based Test Data Generation, 2002.
- No 1000 **Anders Arpteg:** Adaptive Semi-structured Information Extraction, 2002.
- No 1001 **Andrzej Bednarski:** A Dynamic Programming Approach to Optimal Retargetable Code Generation for Irregular Architectures, 2002.
- No 988 **Mattias Arvola:** Good to use! : Use quality of multi-user applications in the home, 2003.
- FiF-a 62 **Lennart Ljung:** Utveckling av en projektivitetsmodell - om organisationers förmåga att tillämpa projektarbetsformen, 2003.
- No 1003 **Pernilla Qvarfordt:** User experience of spoken feedback in multimodal interaction, 2003.
- No 1005 **Alexander Siemers:** Visualization of Dynamic Multibody Simulation With Special Reference to Contacts, 2003.
- No 1008 **Jens Gustavsson:** Towards Unanticipated Runtime Software Evolution, 2003.
- No 1010 **Calin Curescu:** Adaptive QoS-aware Resource Allocation for Wireless Networks, 2003.
- No 1015 **Anna Andersson:** Management Information Systems in Process-oriented Healthcare Organisations, 2003.
- No 1018 **Björn Johansson:** Feedforward Control in Dynamic Situations, 2003.
- No 1022 **Traian Pop:** Scheduling and Optimisation of Heterogeneous Time/Event-Triggered Distributed Embedded Systems, 2003.
- FiF-a 65 **Britt-Marie Johansson:** Kundkommunikation på distans - en studie om kommunikationsmediets betydelse i affärstransaktioner, 2003.
- No 1024 **Aleksandra Tešanovic:** Towards Aspectual Component-Based Real-Time System Development, 2003.
- No 1034 **Arja Vainio-Larsson:** Designing for Use in a Future Context - Five Case Studies in Retrospect, 2003.
- No 1033 **Peter Nilsson:** Svenska bankers redovisningsval vid reservering för befarade kreditförluster - En studie vid införandet av nya redovisningsregler, 2003.
- FiF-a 69 **Fredrik Ericsson:** Information Technology for Learning and Acquiring of Work Knowledge, 2003.
- No 1049 **Marcus Comstedt:** Towards Fine-Grained Binary Composition through Link Time Weaving, 2003.
- No 1052 **Åsa Hedenskog:** Increasing the Automation of Radio Network Control, 2003.
- No 1054 **Claudiu Duma:** Security and Efficiency Tradeoffs in Multicast Group Key Management, 2003.
- FiF-a 71 **Emma Eliason:** Effektanalys av IT-systems handlingsutrymme, 2003.
- No 1055 **Carl Cederberg:** Experiments in Indirect Fault Injection with Open Source and Industrial Software, 2003.
- No 1058 **Daniel Karlsson:** Towards Formal Verification in a Component-based Reuse Methodology, 2003.
- FiF-a 73 **Anders Hjalmarsson:** Att etablera och vidmakthålla förbättringsverksamhet - behovet av koordination och interaktion vid förändring av systemutvecklingsverksamheter, 2004.
- No 1079 **Pontus Johansson:** Design and Development of Recommender Dialogue Systems, 2004.
- No 1084 **Charlotte Stoltz:** Calling for Call Centres - A Study of Call Centre Locations in a Swedish Rural Region, 2004.
- FiF-a 74 **Björn Johansson:** Deciding on Using Application Service Provision in SMEs, 2004.
- No 1094 **Genevieve Gorrell:** Language Modelling and Error Handling in Spoken Dialogue Systems, 2004.
- No 1095 **Ulf Johansson:** Rule Extraction - the Key to Accurate and Comprehensive Data Mining Models, 2004.
- No 1099 **Sonia Sangari:** Computational Models of Some Communicative Head Movements, 2004.
- No 1110 **Hans Nässla:** Intra-Family Information Flow and Prospects for Communication Systems, 2004.
- No 1116 **Henrik Sällberg:** On the value of customer loyalty programs - A study of point programs and switching costs, 2004.
- FiF-a 77 **Ulf Larsson:** Designarbete i dialog - karaktärisering av interaktionen mellan användare och utvecklare i en systemutvecklingsprocess, 2004.
- No 1126 **Andreas Borg:** Contribution to Management and Validation of Non-Functional Requirements, 2004.
- No 1127 **Per-Ola Kristensson:** Large Vocabulary Shorthand Writing on Stylus Keyboard, 2004.
- No 1132 **Pär-Anders Albinsson:** Interacting with Command and Control Systems: Tools for Operators and Designers, 2004.
- No 1130 **Ioan Chisalita:** Safety-Oriented Communication in Mobile Networks for Vehicles, 2004.
- No 1138 **Thomas Gustafsson:** Maintaining Data Consistency in Embedded Databases for Vehicular Systems, 2004.
- No 1149 **Vaida Jakoniené:** A Study in Integrating Multiple Biological Data Sources, 2005.
- No 1156 **Abdil Rashid Mohamed:** High-Level Techniques for Built-In Self-Test Resources Optimization, 2005.
- No 1162 **Adrian Pop:** Contributions to Meta-Modeling Tools and Methods, 2005.
- No 1165 **Fidel Vascós Palacios:** On the information exchange between physicians and social insurance officers in the sick leave process: an Activity Theoretical perspective, 2005.
- FiF-a 84 **Jenny Lagsten:** Verksamhetsutvecklande utvärdering i informationssystemprojekt, 2005.
- No 1166 **Emma Larsdotter Nilsson:** Modeling, Simulation, and Visualization of Metabolic Pathways Using Modelica, 2005.
- No 1167 **Christina Keller:** Virtual Learning Environments in higher education. A study of students' acceptance of educational technology, 2005.
- No 1168 **Cécile Åberg:** Integration of organizational workflows and the Semantic Web, 2005.
- FiF-a 85 **Anders Forsman:** Standardisering som grund för informationssamverkan och IT-tjänster - En fallstudie baserad på trafikinformationstjänsten RDS-TMC, 2005.
- No 1171 **Yu-Hsing Huang:** A systemic traffic accident model, 2005.
- FiF-a 86 **Jan Olausson:** Att modellera uppdrag - grunder för förståelse av processinriktade informationssystem i transaktionsintensiva verksamheter, 2005.
- No 1172 **Petter Ahlström:** Affärsstrategier för seniorbostadsmarknaden, 2005.
- No 1183 **Mathias Cöster:** Beyond IT and Productivity - How Digitization Transformed the Graphic Industry, 2005.
- No 1184 **Åsa Horzella:** Beyond IT and Productivity - Effects of Digitized Information Flows in Grocery Distribution, 2005.
- No 1185 **Maria Kollberg:** Beyond IT and Productivity - Effects of Digitized Information Flows in the Logging Industry, 2005.
- No 1190 **David Dinka:** Role and Identity - Experience of technology in professional settings, 2005.

- No 1191 **Andreas Hansson:** Increasing the Storage Capacity of Recursive Auto-associative Memory by Segmenting Data, 2005.
- No 1192 **Nicklas Bergfeldt:** Towards Detached Communication for Robot Cooperation, 2005.
- No 1194 **Dennis Maciuszek:** Towards Dependable Virtual Companions for Later Life, 2005.
- No 1204 **Beatrice Alenljung:** Decision-making in the Requirements Engineering Process: A Human-centered Approach, 2005.
- No 1206 **Anders Larsson:** System-on-Chip Test Scheduling and Test Infrastructure Design, 2005.
- No 1207 **John Wilander:** Policy and Implementation Assurance for Software Security, 2005.
- No 1209 **Andreas Käll:** Översättningar av en managementmodell - En studie av införandet av Balanced Scorecard i ett landsting, 2005.
- No 1225 **He Tan:** Aligning and Merging Biomedical Ontologies, 2006.
- No 1228 **Artur Wilk:** Descriptive Types for XML Query Language Xcerpt, 2006.
- No 1229 **Per Olof Pettersson:** Sampling-based Path Planning for an Autonomous Helicopter, 2006.
- No 1231 **Kalle Burbeck:** Adaptive Real-time Anomaly Detection for Safeguarding Critical Networks, 2006.
- No 1233 **Daniela Mihailescu:** Implementation Methodology in Action: A Study of an Enterprise Systems Implementation Methodology, 2006.
- No 1244 **Jörgen Skågeby:** Public and Non-public gifting on the Internet, 2006.
- No 1248 **Karolina Eliasson:** The Use of Case-Based Reasoning in a Human-Robot Dialog System, 2006.
- No 1263 **Misook Park-Westman:** Managing Competence Development Programs in a Cross-Cultural Organisation - What are the Barriers and Enablers, 2006.
- FiF-a 90 **Amra Halilovic:** Ett praktikerspektiv på hantering av mjukvarukomponenter, 2006.
- No 1272 **Raquel Flodström:** A Framework for the Strategic Management of Information Technology, 2006.
- No 1277 **Viacheslav Izosimov:** Scheduling and Optimization of Fault-Tolerant Embedded Systems, 2006.
- No 1283 **Håkan Hasewinkel:** A Blueprint for Using Commercial Games off the Shelf in Defence Training, Education and Research Simulations, 2006.
- FiF-a 91 **Hanna Broberg:** Verksamhetsanpassade IT-stöd - Designteori och metod, 2006.
- No 1286 **Robert Kaminski:** Towards an XML Document Restructuring Framework, 2006.
- No 1293 **Jiri Trnka:** Prerequisites for data sharing in emergency management, 2007.
- No 1302 **Björn Häggglund:** A Framework for Designing Constraint Stores, 2007.
- No 1303 **Daniel Andreasson:** Slack-Time Aware Dynamic Routing Schemes for On-Chip Networks, 2007.
- No 1305 **Magnus Ingmarsson:** Modelling User Tasks and Intentions for Service Discovery in Ubiquitous Computing, 2007.
- No 1306 **Gustaf Svedjemo:** Ontology as Conceptual Schema when Modelling Historical Maps for Database Storage, 2007.
- No 1307 **Gianpaolo Conte:** Navigation Functionalities for an Autonomous UAV Helicopter, 2007.
- No 1309 **Ola Leifler:** User-Centric Critiquing in Command and Control: The DKExpert and ComPlan Approaches, 2007.
- No 1312 **Henrik Svensson:** Embodied simulation as off-line representation, 2007.
- No 1313 **Zhiyuan He:** System-on-Chip Test Scheduling with Defect-Probability and Temperature Considerations, 2007.
- No 1317 **Jonas Elmqvist:** Components, Safety Interfaces and Compositional Analysis, 2007.
- No 1320 **Håkan Sundblad:** Question Classification in Question Answering Systems, 2007.
- No 1323 **Magnus Lundqvist:** Information Demand and Use: Improving Information Flow within Small-scale Business Contexts, 2007.
- No 1329 **Martin Magnusson:** Deductive Planning and Composite Actions in Temporal Action Logic, 2007.
- No 1331 **Mikael Asplund:** Restoring Consistency after Network Partitions, 2007.
- No 1332 **Martin Fransson:** Towards Individualized Drug Dosage - General Methods and Case Studies, 2007.
- No 1333 **Karin Camara:** A Visual Query Language Served by a Multi-sensor Environment, 2007.
- No 1337 **David Broman:** Safety, Security, and Semantic Aspects of Equation-Based Object-Oriented Languages and Environments, 2007.
- No 1339 **Mikhail Chalabine:** Invasive Interactive Parallelization, 2007.
- No 1351 **Susanna Nilsson:** A Holistic Approach to Usability Evaluations of Mixed Reality Systems, 2008.
- No 1353 **Shanai Ardi:** A Model and Implementation of a Security Plug-in for the Software Life Cycle, 2008.
- No 1356 **Erik Kuiper:** Mobility and Routing in a Delay-tolerant Network of Unmanned Aerial Vehicles, 2008.
- No 1359 **Jana Rambusch:** Situated Play, 2008.
- No 1361 **Martin Karresand:** Completing the Picture - Fragments and Back Again, 2008.
- No 1363 **Per Nyblom:** Dynamic Abstraction for Interleaved Task Planning and Execution, 2008.
- No 1371 **Fredrik Lantz:** Terrain Object Recognition and Context Fusion for Decision Support, 2008.
- No 1373 **Martin Lundlund:** Assistance Plus: 3D-mediated Advice-giving on Pharmaceutical Products, 2008.
- No 1381 **Håkan Östvall:** Automatic Parallelization using Pipelining for Equation-Based Simulation Languages, 2008.
- No 1386 **Mirko Thorstensson:** Using Observers for Model Based Data Collection in Distributed Tactical Operations, 2008.
- No 1387 **Bahlol Rahimi:** Implementation of Health Information Systems, 2008.
- No 1392 **Maria Holmqvist:** Word Alignment by Re-using Parallel Phrases, 2008.
- No 1393 **Mattias Eriksson:** Integrated Software Pipelining, 2009.
- No 1401 **Annika Öhgren:** Towards an Ontology Development Methodology for Small and Medium-sized Enterprises, 2009.
- No 1410 **Rickard Holsmark:** Deadlock Free Routing in Mesh Networks on Chip with Regions, 2009.
- No 1421 **Sara Stymne:** Compound Processing for Phrase-Based Statistical Machine Translation, 2009.
- No 1427 **Tommy Ellqvist:** Supporting Scientific Collaboration through Workflows and Provenance, 2009.
- No 1450 **Fabian Segelström:** Visualisations in Service Design, 2010.
- No 1459 **Min Bao:** System Level Techniques for Temperature-Aware Energy Optimization, 2010.
- No 1466 **Mohammad Saifullah:** Exploring Biologically Inspired Interactive Networks for Object Recognition, 2011

- No 1468 **Qiang Liu:** Dealing with Missing Mappings and Structure in a Network of Ontologies, 2011.
- No 1469 **Ruxandra Pop:** Mapping Concurrent Applications to Multiprocessor Systems with Multithreaded Processors and Network on Chip-Based Interconnections, 2011.
- No 1476 **Per-Magnus Olsson:** Positioning Algorithms for Surveillance Using Unmanned Aerial Vehicles, 2011.
- No 1481 **Anna Vapen:** Contributions to Web Authentication for Untrusted Computers, 2011.
- No 1485 **Loove Broms:** Sustainable Interactions: Studies in the Design of Energy Awareness Artefacts, 2011.
- FiF-a 101 **Johan Blomkvist:** Conceptualising Prototypes in Service Design, 2011.
- No 1490 **Håkan Warnquist:** Computer-Assisted Troubleshooting for Efficient Off-board Diagnosis, 2011.
- No 1503 **Jakob Rosén:** Predictable Real-Time Applications on Multiprocessor Systems-on-Chip, 2011.
- No 1504 **Usman Dastgeer:** Skeleton Programming for Heterogeneous GPU-based Systems, 2011.
- No 1506 **David Landén:** Complex Task Allocation for Delegation: From Theory to Practice, 2011.
- No 1507 **Kristian Stavåker:** Contributions to Parallel Simulation of Equation-Based Models on Graphics Processing Units, 2011.
- No 1509 **Mariusz Wzorek:** Selected Aspects of Navigation and Path Planning in Unmanned Aircraft Systems, 2011.
- No 1510 **Piotr Rudol:** Increasing Autonomy of Unmanned Aircraft Systems Through the Use of Imaging Sensors, 2011.
- No 1513 **Anders Carstensen:** The Evolution of the Connector View Concept: Enterprise Models for Interoperability Solutions in the Extended Enterprise, 2011.
- No 1523 **Jody Foo:** Computational Terminology: Exploring Bilingual and Monolingual Term Extraction, 2012.
- No 1550 **Anders Fröberg:** Models and Tools for Distributed User Interface Development, 2012.
- No 1558 **Dimitar Nikolov:** Optimizing Fault Tolerance for Real-Time Systems, 2012.
- No 1582 **Dennis Andersson:** Mission Experience: How to Model and Capture it to Enable Vicarious Learning, 2013.
- No 1586 **Massimiliano Raciti:** Anomaly Detection and its Adaptation: Studies on Cyber-physical Systems, 2013.
- No 1588 **Banafsheh Khademhosseini:** Towards an Approach for Efficiency Evaluation of Enterprise Modeling Methods, 2013.
- No 1589 **Amy Rankin:** Resilience in High Risk Work: Analysing Adaptive Performance, 2013.
- No 1592 **Martin Sjölund:** Tools for Understanding, Debugging, and Simulation Performance Improvement of Equation-Based Models, 2013.
- No 1606 **Karl Hammar:** Towards an Ontology Design Pattern Quality Model, 2013.
- No 1624 **Maria Vasilevska:** Designing Security-enhanced Embedded Systems: Bridging Two Islands of Expertise, 2013.
- No 1627 **Ekhlot Vergara:** Exploiting Energy Awareness in Mobile Communication, 2013.
- No 1644 **Valentina Ivanova:** Integration of Ontology Alignment and Ontology Debugging for Taxonomy Networks, 2014.
- No 1647 **Dag Sonntag:** A Study of Chain Graph Interpretations, 2014.
- No 1657 **Kiril Kiryazov:** Grounding Emotion Appraisal in Autonomous Humanoids, 2014.
- No 1683 **Zlatan Dragicic:** Completing the Is-a Structure in Description Logics Ontologies, 2014.
- No 1688 **Erik Hansson:** Code Generation and Global Optimization Techniques for a Reconfigurable PRAM-NUMA Multicore Architecture, 2014.
- No 1715 **Nicolas Melot:** Energy-Efficient Computing over Streams with Massively Parallel Architectures, 2015.
- No 1716 **Mahder Gebremedhin:** Automatic and Explicit Parallelization Approaches for Mathematical Simulation Models, 2015.
- No 1722 **Mikael Nilsson:** Efficient Temporal Reasoning with Uncertainty, 2015.
- No 1732 **Vladislavs Jahundovics:** Automatic Verification of Parameterized Systems by Over-Approximation, 2015.
- FiF 118 **Camilla Kirkegaard:** Adding Challenge to a Teachable Agent in a Virtual Learning Environment, 2016.
- No 1758 **Vengatanathan Krishnamoorthi:** Efficient and Scalable Content Delivery of Linear and Interactive Branched Videos, 2016.
- No 1771 **Andreas Löfwenmark:** Timing Predictability in Future Multi-Core Avionics Systems, 2017.
- No 1777 **Anders Andersson:** Extensions for Distributed Moving Base Driving Simulators, 2017.
- No 1780 **Olov Andersson:** Methods for Scalable and Safe Robot Learning, 2017.
- No 1782 **Robin Keskisärkkä:** Towards Semantically Enabled Complex Event Processing, 2017.
- No 1783 **Daniel de Leng:** Spatio-Temporal Stream Reasoning with Adaptive State Stream Generation, 2017.
- No 1827 **Johan Falkenjack:** Towards a Model of General Text Complexity for Swedish, 2018.
- No 1836 **Magdalena Granäsen:** Exploring C2 Capability and Effectiveness in Challenging Environments: Interorganizational Crisis Management, Military Operations and Cyber Defence, 2019.
- No 1848 **Alachew Mengist:** Methods and Tools for Efficient Model-Based Development of Cyber-Physical Systems with Emphasis on Model and Tool Integration, 2019.
- No 1871 **Klervie Tocze:** Latency-aware Resource Management at the Edge, 2020.
- No 1881 **Chih-Yuan Lin:** A Timing Approach to Network-based Anomaly Detection for SCADA Systems, 2020.

FACULTY OF SCIENCE AND ENGINEERING

Linköping Studies in Science and Technology. Licentiate Thesis No. 1881, 2020
Department of Computer and Information Science

Linköping University
SE-581 83 Linköping, Sweden

www.liu.se