Industrial Control Systems Security: What is happening?

Maryna Krotofil, Dieter Gollmann
Institute for Security in Distributed Applications, Hamburg University of Technology,
21079 Hamburg, Germany

***Abstract*—Increasing awareness of ICS security issues has brought about a growing body of work in this area, including pioneering contributions based on realistic control system logs and network traces. This paper surveys the state of the art in ICS security research, including efforts of industrial researchers, highlighting the most interesting works. Research efforts are grouped into divergent areas, where we add "secure control" as a new category to capture security goals specific to control systems that differ from security goals in traditional IT systems.**

I. Introduction

Critical infrastructure security had become a fashionable topic in the last decade, partly because use of the Internet and use of commodity software brought security challenges to industries that so far had secluded themselves from common IT security threats, partly because the potential impact on society was so large that governments felt that remaining inactive would be negligent. Terms such as ICS or SCADA security entered the discussion. The difference between the two is not always well understood and the terminology is often used inappropriately. Figure 1 explains the distinctions between various types of control systems.

ICS have traditionally been designed for dependability, durability and ease of safe use. Pervasive computerization and automation of control systems has enabled vertical and horizontal systems integration and introduced cyber interdependencies [1]. This became a source of disturbances which are unusual and difficult to foresee. Subtle control loops, cascading failures and malware propagation were the price for increased efficiency. Technology became an enabler of efficiency but also a source of problems. E.g. what used to be an analog sensor has become a high-tech transmitter with multiple wired and wireless communication modes and even a web-server, so that the maintenance staff can take the readings without approaching the device or remotely calibrate it to the process requirements. While security engineers try to limit the numbers of access points, innovative vendors open them up.

Although modernization and exposure to untrusted networks are mentioned as the main reasons for an increased vulnerability of control systems, the danger of insider threats is still underestimated [2] despite the alarm was raised as early as 1998 [3]. The latest cyber-incident made public was an insider incident. Unknown to a technician, his USB-drive was infected with a variant of the Mariposa virus. The infection resulted in downtime and delayed the impacted plant restart by almost three weeks [4]. This shows that relying solely on perimeter protection and network segmentation is a poor strategy and it is required to work towards security in depth.

While in the past, absence of access to the real production systems and network dumps forced ICS research to be based on assumptions, the first facilities have chosen to open their doors to support research projects with real-world data. First analysis has shown that not all suppositions were accurate. Besides, first studies of the process behavior in the presence of intentional manipulations has shown that understanding of physical and control laws is a promising research direction and can be leveraged to achieve processes resilience.

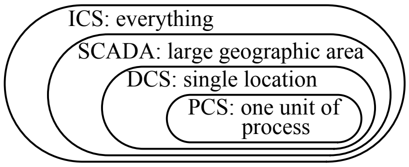

Fig. 1. Initial terminology: ICS – Industrial Control System(s); SCADA – Supervisory Control and Data Acquisition; DCS: Distributed Control System; PCS – Process Control System

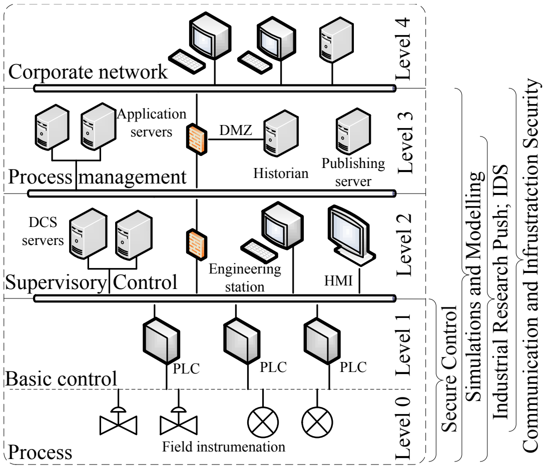

Fig. 2. Paper outline with respect to the ICS reference architecture

In this paper we provide a short but broad overview of the state of the art in ICS security research with a predominant focus on process control systems. We have grouped research efforts into divergent research domains, including a novel research direction which we named "secure control". We have also included the contribution of industrial researchers, which are usually unknown in academic papers, and a brief roundup of advances in modeling and building simulation environments. Figure 2 presents the scope of research sub-areas with respect to an ICS reference architecture. Although it is not possible to include all works done on ICS security, we have selected results which cover the broad range of aspects

978-1-4799-0752-6/13/$31.00 ©2013 IEEE

in the outlined research sub-areas. Beyond the scope of this paper are industrial wireless technologies and works on safety in the context of surviving hazardous conditions.

II. Industrial Research Push

The main goal of industrial researchers' efforts in demonstrating the fragility and insecurity of most ICS field devices is to exert pressure: on one hand on vendors – to introduce a security life-cycle into the design and implementation of field devices, and on the other hand on operators – to introduce proper security policies and replace old equipment with new one which is more secure. The SCADA vulnerabilities search rush was triggered off in 2010 by Project Basecamp [5], an initiative of the security company Digital Bond and a team of volunteer researchers. Whereas some vulnerabilities are real weaknesses in the implementation of security mechanisms (e.g. hardcoded passwords), others are "insecure by design" issues, such as execution of administrative commands without authentication. It would not be possible to give even a half-complete list of discovered vulnerabilities, many of which resulted in the release of ready-to-use exploits and exploit kits. A detailed taxonomy and statistics on discovered ICS vulnerabilities is presented in [6] (status 2012). In [7] the author takes readers along on a journey into the secrets of Schneider Electrics PLC firmware. The result of his efforts was a discovery of 13 hidden accounts which could be exploited for gaining unauthorized access. An approach to discovering backdoors, confidential information and software vulnerabilities in ICS devices is described in [8].

In the past, the reluctance of some vendors to admitting and fixing discovered vulnerabilities resulted in numerous vendor-researcher conflicts, which often ended in releasing an exploit before patch. This resulted in great tension within the researchers-vendors-operators triangle as the latter found themself in a situation with no solution. Attempting to coordinate discovered and reported vulnerabilities with the affected vendor and allow sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to disclosure, ICS-CERT (USA) developed a Vulnerability Disclosure Policy [9]. This initiative stimulated "responsible discloser" behavior thereby reducing the number of unscrupulous exploit releases before patch.

A study [10] is the first work to debunk a popular folk myth that ICS are never connected to the Internet. The researcher used the search engine SHODAN [11] to map industrial system devices and systems which are directly connected to the Internet. Discovered connections were logged over time and visualized alongside with relevant vulnerability information from the computer security community thus presenting a credible global view of ICS connectivity and vulnerability. Everyone who wishes can use a provided "cheatshit" for easy searching (e.g. Schneider PLC). Project SHINE [4] picked up the baton and compiled a list of devices with control systems impact, such as smart meters, traffic control and railway signaling systems, elevators, etc. In some instances discovered devices have weak, non-existent or default login credentials.

No paper on ICS security would be complete without mentioning Stuxnet. Although the most detailed dossier was published by Symantec [12], the topmost effort into "deciphering" the PLC-related part of malware was contributed by Ralph Langner. As his analysis progressed, Langner provided meticulous detailing on Stuxnet payload in his blog [13], including criticism on multiple inaccuracies in the Symantec report. Although it was widely believed that "Stuxnet-like" malware invasion was inevitable, it turned that Stuxnet sophistication is not necessarily required for compromising control hardware while achieving similar results [14].

III. Communication and Infrastructure Security

Communication protocols enable interaction between cyber-physical components. The state of the facility depends on the process and management data stored in and transmitted through the communication infrastructure. The key to handling the data was the establishment of a transparent information flow inside of an automation system [15]. Shift toward vertical and horizontal integrations as well as tunneling serial field protocols over the Ethernet brought with it tighter, more complex and more extensive interdependencies along with increased risks and greater requirements to security.

An exhaustive taxonomy of architectural, software-, protocols- and policies related SCADA vulnerabilities, attack scenarios and security countermeasures is presented in [16]. Specific vulnerabilities of Modbus and DNP3 protocols are listed along with the associated dangers if they are being exploited. A catalogue of possible attack scenarios includes manipulation of process and management data at all levels of the ICS reference architecture. Security analysis of further field protocols, not only serial and open source, but also Ethernet-based and proprietary protocols is discussed in [17]. Another contribution of the paper is a security analysis of the field devices, such as smart sensors (transmitters) and actuators. They are usually based on proprietary firmware and found at the lowest layer of the automation reference architecture. The authors illuminate the perils of information leakage and tampering risks as well as the dangers of exploiting software vulnerabilities and debugging interfaces.

A taxonomy of the attacks on the predominant protocol in the energy sector DNP3 is presented in [18]. In total, 28 possible attacks and 91 attack instances based on communication layers were identified. The majority of the attacks lead to serious consequences such as loss of situational awareness and loss of control. As a possible countermeasure, a DNPSec framework could be deployed [19] which enables confidentiality, integrity, and authenticity in the DNP3 protocol. However, the proposed concept was not tested or simulated. In [20] the author elaborates on vulnerabilities in Modbus TCP and IEC 61850. The paper addresses two types of attacks against protocol implementations: flawed or missing cryptographic protection and memory corruption vulnerabilities. Both protocols are predominately coded in C/C++ and subject to multiple protocol specific and generic memory corruptions. Pure-data attacks on Modbus allow overwriting non-control data, which contribute to the actual computations done by control applications. Such attacks provide a staging post for more complex attacks against physical processes and equipment. One possible mitigation technique is to incorporate security features for integrity, authentication, and anti-replay protection as proposed in [21]. However the success of the presented cryptographic security mechanisms greatly depends on the preservation of secrecy of the shared keys. One approach to combating memory corruption attacks on Modbus control systems is proposed in [22]. In [23] and [24] the authors present a set of theoretically proven attacks on PROFINET IO and PROFIsafe. In both cases it is shown that taking control of a PROFINET/PROFIsafe node without any of the peers detecting the attack is possible.

A possible objective of targeted cyber attacks on industrial facilities is physical damage to equipment or sabotage of physical processes which those systems monitor and control. Depending on the equipment specifications and underlying physics, there is a variety of techniques which can be applied to achieve a destructive goal. A taxonomy of such techniques, with examples, is presented in [25]. Ladder logic, operator console and observations of the process reactions provide valuable information on harmful or unsafe operating modes. One of the most famous examples of control hardware vulnerabilities – the Aurora vulnerability – is explained in [26]. An attacker equipped with knowledge of the connection and protection details of an electrical power generator can provoke damage to the facility. In order to "automate" her attacks, an adversary might decide to design a specific malware, which takes advantage of underlying protocol vulnerabilities. SCADA malware designed in [27] proves that autonomous ICS attacks are feasible. Considerations on constructing a dynamic payload for PLC malware are shared in [28].

Until recently there were no works based on empirical data analysis from real-world ICS facilities. In the absence of insights into real control domain data traces it was widely believed that this traffic was fully deterministic and periodic. A "first look" into SCADA traffic through flow-based analysis of network traces is provided in [29]. Although, as expected, data were predominantly generated in a periodical fashion and exhibited regular time series, it was observed that changes do occur. This finding is explained in [30]. Further analysis of data dumps has shown that the major part of a control communication map (90%) is built within 5 minutes of the network trace. However, devices that do not directly participate in the production process contribute to the newly discovered traces.

IV. Advances in Simulations and Modeling

Apart from the prevalence of proprietary firmware and protocols, the major challenge of ICS security is the lack of efficient ways conducting safe and practical experiments to measure the impact of cyber attacks on machinery and physical processes. This is related to the high complexity of such systems and their interaction with real physical phenomena. Conducting experiments on real systems is not safe especially while testing damaging manipulations. Moreover, it would be difficult and costly to reproduce such tests to confirm the results. The alternative is to use models of the physical processes and to run software-based experiments, e.g. in Matlab. On the other hand, although it is safe to investigate ICS communication infrastructure under attacks, it is challenging and expensive to recreate the distributed nature of such systems. There are a few ways to overcome this limitation, which we present in this section.

An overview of different approaches to building an experimental testbed is presented in [31]. In general, realistic, hybrid and simulated frameworks are possible. High fidelity of a fully realistic test environment like the one presented in [32] is counterbalanced by its poor flexibility and high maintenance costs. On the contrary fully simulated environments do not capture the representative communication and behavioral patterns as well as not allowing experiments with real malware. The prevalent hybrid approach implies integration of the simulated and real components, and provides a cost- and manpower-effective solution. An advanced method of hybrid experimental setup is put forward in [31] in which Matlab Simulink is used for simulating physical components and an emulation environment Emulab recreates the cyber components of the ICS. Such an approach provides high accuracy of the experiments as well as flexibility and scalability. Among the disadvantages are high fixed manpower and monetary costs, thus making this approach unsuitable for small research groups or short-term research projects.

Modeling and security analysis of physical processes might be the most challenging implementation issue for IT-security scientists due to lack of process and control engineering knowledge. Although mathematical process models with program listings exist [33], [34], a lot of work is still needed to transfer models into Matlab Simulink code and obtain results meaningful for the research objective. Moreover, if a detailed description of process dynamic does not exist, analysis and interpretation of model behavior might be very cumbersome. On this premise, the Tennessee Eastman Challenge Process, a very well studied process control problem with available Matlab code, was a first candidate for security studies [31], [35], [36]. Several models of power plants models are listed in [37]. It is also possible to derive customized equations and Matlab models for the process of interest as it is done in [38]. However, this approach requires consulting external process engineers and substantial implementation and validation efforts to confirm the correctness of model behavior, especially in abnormal situation. Comparison of measured and simulated grid performance in [39] demonstrates how drastic a difference between the two could be.

For some works, recreating accurate ICS traffic patterns is crucial for simulation and result validation. In [40] authors verified whether models used to describe traditional network patterns can be also applied to SCADA traffic. Analysis of two real-world SCADA traffic traces revealed that SCADA networks present neither diurnal patterns of activities nor self-similar correlations in the time series common to traditional IT networks. Results regarding tail behavior of connection size distributions were not always conclusive. In summary, existing traffic models cannot be easily applied to SCADA traffic.

Formal methods provide a foundation for specification, development and verification of software and hardware systems and thus are important in any engineering discipline. Since ICS security is rather a new research arena, there is still a lack of theoretical basis for formal representations of ICS for security studies. In [41] the authors propose a formal methodology for evaluating the security of multilayer SCADA protocols in the context of Modbus TCP. An ontological framework which permits formal representation of control elements and process under control is presented in [42]. The authors also derived a fault diagnosis algorithm which leverages the ontological model to fuse cyber security relevant components with process control elements. The algorithm identifies process anomalies and maps them either to a traditional fault source or to a component under cyber attack. A formal adversary capability model for SCADA environment is presented in [43]. This model takes into account important communication constraints of SCADA environments which limit the attacker's capacity.

V. Secure Control

The security goal in the traditional IT domain is the protection of information, be it data in storage or in transit. The security goal in the ICS realm is to protect the operations so that in the words of Ross Anderson, "the electricity continues to come out of the wall socket, regardless of the attempts of either Murphy of Satan to interrupt the supply" [44]. In this respect considering ICS security as solely an IT-related problem is not helpful. Encryption and digital signatures are powerless if the control algorithm was modified by a "trusted" entity. Incorporating information about physical and control laws is a novel security research challenge which could be summarized as *secure control* using a term coined at [45].

A good starting point for a new research initiative is the establishment of an applicative vocabulary. We adapt translation of traditional security properties into the process control world from [45]. **Availability** is interpreted as the capacity to maintain operations by preventing or surviving DoS attacks to the information collected by the sensor, commands given by controllers, and physical actions taken by the actuators. Due to hard real-time requirements in the control domain, timeliness [46] can be considered as an availability issue. Process data are only valid for a short time and might become irrelevant if arriving too late. The same applies to the scheduling of needed task actions. **Integrity** is interpreted as the ability to prevent, detect and survive deception attacks. Deception is the result of an authorized party (e.g. controller) receiving false data and believing it to be true. The security property which reflects the trustworthiness of the assertion is called **veracity** in [47]. In terms of control systems, veracity translates into ensuring sensors faithfully capturing measurements of process state or controllers issuing truthful commands as a result of control algorithm execution. Veracity also applies to process information storage as many advanced control algorithms take their decisions based on the historical dynamic of process data. **Confidentiality** in terms of secure control should prevent an adversary from inferring the state of the physical system by eavesdropping on the communication channel between the sensors, controllers and actuators. In [46] security goals of ICS are supplemented with **graceful degradation** meaning ability to keep the attack impact local avoiding cascading failure.

Better understanding which parameters influence the success and consequences of attacks provides an insight into the adversary's decision making about attack strategy and form a foundation for risk assessment at process control environments. As demonstrated in [48] the effectiveness of a remotely executed cyber attack depends on multiple parameters. In the scenario presented, the attacker issues bogus Modbus packets to three different valves at a boiling plant trying to keep them in a certain position. The results showed that whereas packet losses did not have a significant effect, networks delays and high background traffic were beneficial to the physical process when confronted with a cyber attack. However, the adversary's success is very dependent on the speed of the valve: slow valves are more vulnerable. PLC task scheduling had a major impact on the attack outcome. The shorter the control cycle, the less successful the attack is. This is intuitive: bogus packets arrive at a low "rate" thus providing the PLC with an opportunity window of few ms to bring the valve back into the right position. The main take away from the work is that certain parameters as valve speed and PLC task scheduling could be adopted at the design phase to yield a more resilient physical process.

Another approach to reasoning about attacks and their consequences is analysis of process design resilience. The ability of a chemical reactor system to withstand process manipulations is studied in [35] and [49]. The attacker is assumed being able to compromise only one sensor or actuator at a time. The analysis shows that DoS attacks has relatively little impact on a system in a steady state. The adversary needs to follow different strategies while targeting plant safety or plant economy (product quality or cost). If the attacker is not aware of plant dynamics and attacks a random sensor or controller, she might damage the production, but not necessarily succeed in bringing the system into an unsafe state as the attacks on different components and control loops take less time to upset the process than on others. This information is important for the plant operator for prioritizing security budget expenditures, e.g. investing into tamper resistant sensor or actuators whose performance have a crucial influence on plant resilience.

Control loops, whose performance have a considerable impact on plant resilience can be hardened with control laws that are robust against malicious actions and are able to change their control strategy based on the detected attack scenario. The calculus proposed in [50] enables synthesizing a causal feedback controller for discrete-time, dynamical linear systems so that it meets high safety constrains in the presence of DoS attacks.

Subverted field devices can generate erroneous input data for control algorithms and ICS applications thereby causing generation of logs and automated actions which do not reflect the real situation in the field. Therefore ensuring the veracity of process measurements is the cornerstone requirement for resilient process control. The laws of physics may help the defender to identify impossible or implausible sensor readings. In [38] authors propose to make use of indirect nonlinear relationships between process variables in a biochemical process to ascertain the plausibility and thus trustworthiness of observed readings. This is achieved through the use of suitable proxy measurements. A way to achieve a similar goal utilizing already available measurements and thus minimizing the re-engineering efforts is put forward in [36].

VI. Intrusion Detection

A significant effort on securing ICS is concentrated on intrusion detection solutions. The predictable nature of SCADA traffic and relatively static network topology can be leveraged to detect anomalies whereas known legitimate control sequences/codes and unsafe states make them also suitable for successful deployment of a signature based IDS. At the time of this paper submission we identified more than 35 different approaches to intrusion detection in the control systems domain, excluding works on sensor manipulation detection. We could categorize them into host-, network- and information-based. Into information-based category we attribute techniques which use data or information about the system, e.g. logs or knowledge about critical states of the physical system. However, the success of information-based IDS fully relies on the veracity of the analyzed information. The main shortcoming of some works is obscure justification of chosen approach and missing elaboration on implementation, limitations and simulation results. This makes it difficult to assess the relevance and value of the work. Below we present selected intrusion detection approaches, which take advantage of different specifics of the ICS environment and whose performance was validated through adequate simulations.

A taxonomy of SCADA-specific IDS is presented in [39]. Through resorting to the classic works in the standard IT field and comprehensive analysis of SCADA specifics, the authors derived dimension of taxonomy, multiple features for comparison and evaluation criteria of the approaches. The work is finalized with a survey of 9 up-to-date (status 2010) IDS.

While most research efforts are limited to test environments and simulated data, [51] is a notable exception as this work is based on data from a real-world facility. Moreover, the effectiveness of the chosen approach as well as obtained results are validated with the facility's stakeholders. The proposed methodology aims at identifying process-related threats caused by the activity of users through mining SCADA event logs. Such threats take place when an attacker manages to gain valid user credentials or a legitimate user makes an operational mistake. It is concluded that accurate and effective data mining is not possible without stakeholders' knowledge of plant operations and without including "process knowledge" into the mining algorithm. Moreover, the threshold for extracting anomalous events has to be adjusted dynamically based on the "business" of the day. The feasibility to generalize the approach was evaluated with stakeholders from other facilities. An individual threat analysis and logs preprocessing would be always required, but the approach is believed to be transferable.

The periodicity feature of Modbus TCP traffic allows modeling industrial communication channels with deterministic finite automaton (DFA). The benefits of the DFA-based approach to detecting anomalies in Modbus networks is explored in [52]. Deep packet inspection of about 100 messages is sufficient for constructing the channel's DFA. The approach was tested on a real production system showing low false positive rate. However, the solution was only tested in the presence of the anomalies caused by inaccurate operator actions as opposed to malicious actions.

A signature-based IDS for detecting critical states of a control system [53] make a use of explicit knowledge of the SCADA system to generate a System Virtual Image. The work rests on the assumption that single packet inspection does not provide a defense against complex attacks. An adversary can send a set of commands that are legal if considered in isolation, but interfere with the correct behavior of the system when executed together. The overall system is decomposed into subsystems to the desired level of granularity and is monitored by local IDS. A critical state analyzer identifies whether the state of a virtual image matches any signature from the database of unsafe states. The IDS is capable of semi-real-time critical state detection mainly retarded by the analysis of critical state rules.

A human-assisted intrusion detection technique is proposed by [54]. In this approach, security related events that occur in a control space are reduced into quantitative metrics and visual images understandable by process operators based on which they can assess whether a computer network attack is taking place and call for IT-support. Process perturbance caused by malicious activity would require specific actions to stabilize the process, e.g. neutralization of a DoS attack. However, the proposed approach does not provide real-time detection. For usability reasons only the most critical events or suspicious activities weighted over time will trigger an alarm on the operator console. By the time of detection the attacker might have already succeeded in her mission.

The mirage approach is a military technique to deliberately mislead the adversary thereby causing her to take specific actions. The applicability of this technique in the ICS domain is explored in [55]. The main idea is to enable a defender to influence an attacker's target selection process and pilot it towards a simulated physical process and equipment. The generated malicious network traffic facilitates detection of the ongoing intrusion. Besides, the intrusion is detected upon deviation of simulated environmental variables from safe values.

Several n-gram-based algorithms for network based anomaly detection for binary protocols are evaluated in [56]. Both traditional IT and ICS network data were used for the analysis. An industrial data set was collected at the real-world industrial control network and included traces of Modbus TCP. Analysis reveals that evaluated algorithms based on n-gram analysis exhibits poor performance (detection and false positive rate) when analyzing even moderately variable traffic. Therefore this method is not effective for WEB and LAN datasets. In contrast n-gram-based algorithm for anomaly detection can be potentially deployed in a real industrial environment for Modbus protocol. This is explained by a low variability of field traffic.

VII. Conclusion

The current state of ICS security is somewhat shaky. On one hand, most of the software, hardware and communication protocol vulnerabilities are well known and understood. On the other hand, security requirements and proposed solutions are often beyond the technical capabilities of legacy systems and/or not economically feasible. Even installing available patches is impracticable in certain industries (e.g. pharmaceutical), as it would require a lengthy and expensive plant recertification process. Such companies have no choice but to rely on basic IT-security protection, making plant operation a high risk engineering practice rather than a science-based engineering discipline. One solution to this situation would be to allow recertification of affected subsystems only. Introducing robust control laws and/or refinement of infrastructure parameters is a plausible solution for protecting legacy systems as it would not require hardware replacement.

Physical parameters are unique to each individual facility. To execute a meaningful targeted attack, the adversary has to learn about the system first. In this regard, targeted attacks are likely to precede with silent espionage attacks to steal engineering documentation [57].

Despite of advances in ICS security research, there are still many open questions. One is the analysis of IDS performance during alarm flooding caused by abnormal situations. Abnormal situations comprise a range of minor to major process disruptions in which operations personnel have to intervene to correct problems with which the control systems can not cope. This is a non-trivial problem with no effective solution at the moment [58]. Another challenge is the accurate identification of the cause for process perturbation so that appropriate correction measures can be taken. A clogged dirty valve does not necessary mean a DoS attack as leakage of the valve does not mean that fluid dynamic was intentionally manipulated. Correlating logs from asset management systems (about the “health” of the installation), security systems and process information would greatly facilitate root cause analysis.

References

[1] S. Rinaldi, J. Peerenboom, and T. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies,” *Control Systems*, vol. 21, no. 6, pp. 11 –25, 2001.

[2] D. Gollmann, “From insider threats to business processes that are secure-by-design,” in *INCoS*, 2011, p. 627.

[3] E. Byres, “Network secures process control,” *InTech Magazine*, 1998.

[4] “ICS-CERT Monthly Monitor,” October–December 2012.

[5] “Project Basecamp,” http://www.digitalbond.com/tools/basecamp, 2011.

[6] G. Gritsai et al., “SCADA safety in numbers V1.1*,” Positive Technologies, 2012.

[7] R. Santamarta, “Reversing industrial firmware for fun and backdoors I,” 2011.

[8] ——, “HERE BE BACKDOORS: A jorney into the secrets of industrial firmware,” *Black Hat USA*, 2012.

[9] “Vulnerability disclosure policy,” http://ics-cert.us-cert.gov/ics-cert/disclosure.html, ICS-CERT(USA), 2012.

[10] É. P. Leverett, “Quantitatively assessing and visualising industrial system attack surfaces,” Master’s Thesis, Uni. of Cambridge, UK, 2011.

[11] J. C. Matherly, “man SHODAN,” http://www.shodanhq.com/help, 2009.

[12] N. Falliere, L. O. Murchu, and E. Chien, “W32.Stuxnet Dossier,” Symantic Security Response, Tech. Rep., 2010.

[13] R. Lagner, “Blog,” http://www.langner.com/en/blog/, 2010.

[14] D. Beresford, “Exploiting Siemens Simatic S7 PLCs,” *Black Hat USA*, 2011.

[15] T. Sauter, S. Soucek, W. Kastner, and D. Dietrich, “The evolution of factory and building automation,” *Industrial Electronics Magazine, IEEE*, vol. 5, no. 3, pp. 35–48, 2011.

[16] I. N. Fovino, A. Coletta, and M. Masera, “Taxonomy of security solutions for the SCADA sector,” ESCoRTS, Deliverable: D22, Version:1.1, 2010.

[17] M. Sundell et al., “White paper on industrial automation security in fieldbus and field device level,” 2011.

[18] S. East, J. Butts, M. Papa, and S. Shenoi, “A taxonomy of attacks on theDNP3 protocol,” 2009, pp. 67–81.

[19] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, “DNPSec: Distributed network protocol version 3 (DNP3) security framework,” in *Advances in CISSE*, 2006, pp. 227–234.

[20] J. Rrushi, “SCADA protocol vulnerabilities,” ser. LNCS, 2012, vol. 7130, pp. 150–176.

[21] I. Fovino, A. Carcano, M. Masera, and A. Trombetta, “Design and implementation of a secure modbus protocol,” 2009, pp. 83–96.

[22] C. Bellettini and J. Rrushi, “Combating memory corruption attacks on scada devices,” in *CIP II*, 2009, pp. 141–156.

[23] J. Åkerberg and M. Björkman, “Exploring security in PROFINET IO,” in *COMPSAC*, 2009, pp. 406–412.

[24] ——, “Exploring network security in PROFIsafe,” in *SAFECOMP*, 2009, pp. 67–80.

[25] J. Larsen, “Breakage,” *Black Hat USA*, 2007.

[26] M. Zeller, “Myth or reality - does the aurora vulnerability pose a risk to my generator?” in *Annual Conference for Protective Relay Engineers*, 2011, pp. 130 –136.

[27] A. Carcano, I. N. Fovino, M. Masera, and A. Trombetta, “SCADA malware, a proof of concept,” in *CRITIS*, 2008, pp. 211–222.

[28] S. McLaughlin, “On dynamic malware payloads aimed at programmable logic controllers,” in *HotSec*, 2011.

[29] R. R. R. Barbosa, R. Sadre, and A. Pras, “A first look into SCADA network traffic,” in *NOMS*, 2012, pp. 518–521.

[30] D. Hadžiosmanović, D. Bolzoni, S. Etalle, and P. H. Hartel, “Challenges and opportunities in securing industrial control systems,” in *COMPENG*, 2012, pp. 1–6.

[31] B. Genge, C. Siaterlis, I. N. Fovino, and M. Masera, “A cyber-physical experimentation environment for the security analysis of networked industrial control systems,” 2012, vol. 38, no. 5.

[32] I. Fovino, M. Masera, L. Guidi, and G. Carpi, “An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants,” in *Human System Interactions*, 2010, pp. 679 –686.

[33] J. J. Downs and E. F. Vogel, “A plant-wide industrial process control problem,” 1993, vol. 17, no. 3, pp. 245–255.

[34] R. Bell and K. Åström, “Dynamic models for boiler-turbine-alternator units: Data logs and parameter estimation for a 160 mw unit,” 1987.

[35] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, “Attacks against process control systems: risk assessment, detection, and response.” in *ASIACCS*, 2011, pp. 355–366.

[36] T. McEvoy and S. Wolthusen, “A plant-wide industrial process control security problem,” in *CIP V*, 2011, pp. 47–56.

[37] B. Genge, I. Nai Fovino, C. Siaterlis, and M. Masera, “Analyzing cyber-physical attacks on networked industrial control systems,” in *Critical Infrastructure Protection V*, 2011, pp. 167–183.

[38] T. McEvoy and S. Wolthusen, “Detecting sensor signal manipulations in non-linear chemical processes,” in *CIP IV*, 2010, vol. 342, pp. 81–94.

[39] B. Zhu and S. Sastry, “SCADA-specific intrusion detection/prevention systems: a survey and taxonomy,” in *WSCS*, 2010.

[40] R. R. R. Barbosa, R. Sadre, and A. Pras, “Difficulties in modeling SCADA traffic: A comparative analysis,” ser. LNCS, vol. 7192, 2012, pp. 126–135.

[41] J. Edmonds, M. Papa, and S. Shenoi, “Security analysis of multilayer SCADA protocols,” in *Critical Infrastructure Protection*, 2007, pp. 205–221.

[42] J. Hieb, J. Graham, and J. Guan, “An ontology for identifying cyber intrusion induced faults in process control systems,” in *Critical Infrastructure Protection III*, 2009, pp. 125–138.

[43] T. R. McEvoy and S. D. Wolthusen, “A formal adversary capability model for SCADA environments,” in *CRITIS*, 2011, pp. 93–103.

[44] R. Anderson and S. Fuloria, “Security economics and critical national infrastructure,” in *Economics of Information Security and Privacy*, 2010, pp. 55–66.

[45] A. A. Cárdenas, S. Amin, and S. Sastry, “Secure control: Towards survivable cyber-physical systems,” in *WCPS*, 2008, pp. 495–500.

[46] B. Zhu, A. Joseph, and S. Sastry, “A taxonomy of cyber attacks on SCADA systems,” in *iThings/CPSCom*, 2011, pp. 380–388.

[47] D. Gollmann, “Veracity, plausibility, and reputation.” ser. LNCS, vol. 7322, 2012, pp. 20–28.

[48] B. Genge, C. Siaterlis, and M. Hohenadel, “Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems,” *IJCCC*, vol. 7, no. 4, pp. 673–686.

[49] Y. Huang, A. Cardenas, S. Amin, S.-Z. Lin, H.-Y. Tsai, and S. S. Sastry, “Understanding the physical and economic consequences of attacks against control systems.” *IJCIP*, vol. 2, no. 3, pp. 72–83, 2009.

[50] S. Amin, A. A. Cárdenas, and S. Sastry, “Safe and secure networked control systems under denial-of-service attacks.” ser. LNCS, 2009, pp. 31–45.

[51] D. Dina Hadžiosmanović and D. Bolzoni and P. H. Hartel, “A log mining approach for process monitoring in SCADA,” *IJIS*, vol. 11, pp. 231–251, 2012.

[52] N. Goldenberg and A. Wool, “Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems,” *IJCIP*, no. 0, 2013.

[53] I. Fovino, M. Masera, M. Guglielmi, A. Carcano, and A. Trombetta, “Distributed intrusion detection system for SCADA protocols,” in *Critical Infrastructure Protection IV*, 2010, pp. 95–110.

[54] M. Naedele and O. Biderbost, “Human-assisted intrusion detection for process control systems,” in *ACNS*, 2004, pp. 216–225.

[55] J. L. Rrushi, “An exploration of defensive deception in industrial communication networks,” *IJCIP*, vol. 4, no. 4, 2011.

[56] D. Hadžiosmanović, L. Simionato, D. Bolzoni, E. Zambon, and S. Etalle, “N-gram against the machine: On the feasibility of the n-gram network analysis for binary protocols,” ser. LNCS, vol. 7462, 2012, pp. 354–373.

[57] “ACAD/Medre.A: 10000s of AutoCAD designs leaked in suspected industrial espionage,” ESET, Tech. Rep., 2012.

[58] “Abnormal Situation Management,” http://www.asmconsortium.net.