Demonstrating the feasibility of a new security monitoring framework for SCADA systems

Pedro Yuri Arbs Paiva
Divisão de Engenharia Eletrônica
Instituto Tecnológico de Aeronáutica
São José dos Campos, Brasil
Email: paiva@ita.br

Osamu Saotome
Divisão de Engenharia Eletrônica
Instituto Tecnológico de Aeronáutica
São José dos Campos, Brasil
Email: osaotome@ita.br

Christof Brandauer
Advanced Networking Center
Salzburg Research Forschungsgesellschaft
Salzburg, Austria
Email: christof.brandauer@salzburgresearch.at

***Abstract*—The project SCISSOR (Security in Trusted SCADA and Smart Grids) aims to improve the security of SCADA systems (Supervisory Control and Data Acquisition) by collecting and analyzing heterogeneous sources of data. The framework is composed by four layers, which collect, parse and aggregate the data that will be used for correlation and event detection, generating alerts on a human-machine interface. The purpose of this paper is to present the architecture, illustrating with an example that provides a simple understanding in order to demonstrate its applicability. Despite the choice of some constraints here, we argue that the flexibility and scalability factors allow more sophisticated modules to be inserted. This simplification restricts the sensors to a few types that have a natural correlation. Furthermore, a statistical predictor will play the role of the SIEM (Security Information and Event Management) module.**

***Index Terms*—cyber-physical systems, security, control, critical infrastructure**

I. Introduction

SCADA systems (Supervisory Control and Data Acquisition) are used to collect data from remote sensors and control industrial processes or those that involve critical infrastructures such as power generation, nuclear power plants, refineries and water distribution. A SCADA system performs centralized monitoring and based on information received (e.g. sensors and log data), it generates control signals automatically or activated by human operators. From these commands, local devices can trigger actuators, collect sensor data and monitor the local environment [1].

Figure 1 depicts an ICS (Industrial Control Systems) general layout; levels 0, 1 and 2 comprise the SCADA system. In this topology, there is a control center that gathers all the information generated by the subsystems, displaying them on the HMI and storing the logs in databases. It is also possible to take control actions, like adjusting set-points.

Although SCADA systems have been designed to control and monitor critical infrastructures, they lack security and have several vulnerabilities that can be exploited by threats and cyber-criminals [2]. Due to its relevance, this topic has drawn attention in the last decade and it is still under discussion in academia and industry. There are plenty of works that survey security threats and vulnerabilities in ICS/SCADA [3]–[6] as well as those that attempt to measure the level of security and the effectiveness of mitigation actions [7]–[10].

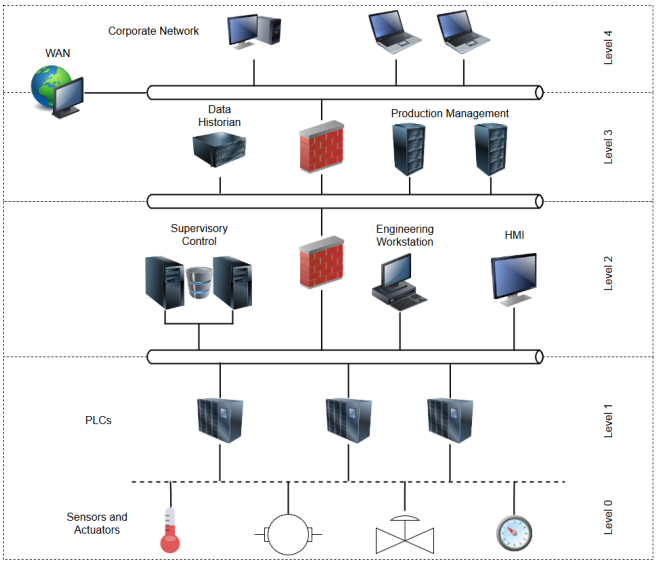


Fig. 1: ICS architecture

The ideal solution, however, would require the redesigning of all ICS systems, which is not possible in practice. Other approaches have been proposed to enhance the security level in industrial systems, but without the need for a redesign. In [11], it processes SCADA logs in order to detect possible threats. Another kind of strategy is the one based on network monitoring. There are more recent works [12], [13] based on this approach, which seeks bad-behavior in network traffic and protocol packets. Lastly, monitoring at process level can also be applied for surveillance and detection. The architecture in [14] explores the real-time characteristic of the plant and can detect abnormal situations regarding the physical system. In [15], the proposed framework tracks process variables through the network and applies monitoring rules for event detection.

Each technique by itself, however, has some weaknesses that could be diminished against their combination in a more effective fashion. Even though log mining has potential to extract a bunch of information from the system, it could be deceitful when the attacker has the ability to fake information. Network monitoring hides, somehow, the physical processes beneath it, which can hedge the system vision.

In this paper, we present SCISSOR (Security in Trusted SCADA and Smart-Grids), a new framework for ICS/SCADA security enhancement. We argue that the methods discussed previously can be put together to yield a more comprehensive solution. Furthermore, we demonstrate part of the framework's capability making use of a simplified version, with a reduced number of components. The rest of the paper is as follows: in section II we discuss deeper the security issues in SCADA systems; section III contains a detailed description of the SCISSOR architecture; in section V we show the cyber-physical scenario chosen; section VI is about the method used in the SIEM module and the last sections are results and discussion.

II. Security issues

Industrial control systems demand high reliability and availability, especially when they are applied to critical infrastructures, such as SCADA systems do. As they are associated with physical processes, in most cases failures and delays can not be tolerated, because the consequences would impact negatively human lives and the environment.

Nevertheless, security in these systems has not been considered a prominent issue at the beginning. A common belief was that of the security through obscurity, which is built on some assumptions [5], [16]:

- Physical isolation between the internal network and the Internet
- Use of proprietary protocols
- Non-standard software and hardware
- Restricted physical access

Due to the distributed nature of critical infrastructures, many services must communicate with spatially separated sites. The use of Internet introduces, therefore, inherent risks and exposes the system to the outside world. Adopting standard network protocols (Ethernet, TCP/IP, etc) and the increasing number of IoT devices present in those plants reinforce the non-isolation factor [5].

Whereas moving towards the use of standard hardware and software is a trend, at the other hand they come with known vulnerabilities [9], [16], which can be exploited by hackers and attackers. Moreover, zero day exploits, which are attacks against publicly unknown vulnerabilities, are especially dangerous because of their unpredictability.

A series of cyber attacks targeting ICS (Industrial Control System) have been reported in the past years. According to IBM research report on ICS [17], the number of attacks per year increased by about 100 percent from 2013 to 2015. Kaspersky report [18] showed that the number of ICS vulnerabilities by year increased from 19 in 2010 to 189 in 2015, and from those in 2015, 49% are considered critical and 42% medium risk.

One of the most notorious SCADA malware, Stuxnet was first observed in 2010 and had supposedly infected a uranium-enrichment plant in Iran. It was specifically created to infect industrial control systems, modifying code on programmable logic controllers (PLC) [19]. Stuxnet is a very complex worm and exploits four zero-day vulnerabilities in Windows OS and Siemens PLC. It enters a system via USB stick and can spread itself through the network, infecting other Windows machines. It then changes the code on PLCs, in order to provide a false view of the system while tearing it apart [20].

III. Architecture

The SCISSOR project seeks to circumvent the security issues in SCADA systems, however, without the need to modify the original plant, innovating through a complementary approach whose strategy is to create a structure that encompasses the system. Thus, the goal is "to create an end-to-end, multi-layer holistic security monitoring framework that includes encryption of communications and access control support" [21]. The framework is structured in four layers, as shown in figure 2.

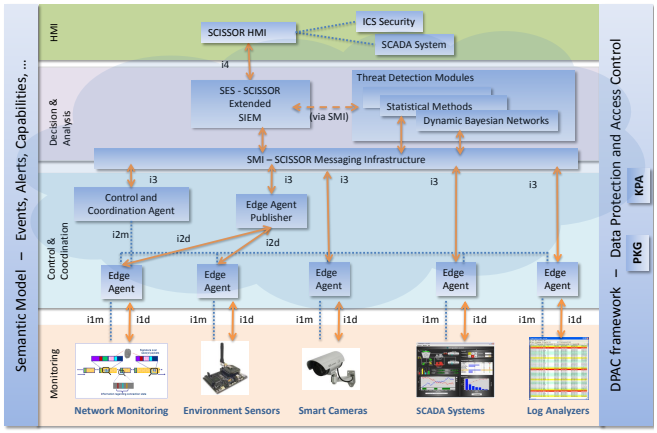


Fig. 2: SCISSOR layered architecture (from [22])

A. Monitoring Layer (ML)

This layer provides an interface with the physical world and other systems, defining a "standard way of integrating any type of monitoring element and connecting them to the SCISSOR framework" [21]. It is designed to collect data from traffic probes (network monitoring), environment sensors, smart cameras and SCADA logs.

B. Control and Coordination Layer (CCL)

The role of CCL is to decouple the monitoring layer from the decision and analysis layer. It delivers data from monitoring elements (previously collected by the ML) in a SCISSOR unified format. Its two main functions can be summarized as:

- to ingest raw data from the monitoring elements, preprocess it and forward to the relevant analysis modules;
- to provide means for implementing dynamic adaptations of the data acquisition process and mitigation actions.

Figure 3 shows the CCL in detail, its interfaces and the composition of an Edge Agent (EA). A feature of the SCISSOR framework is the development of a distributed system

based on decentralization. Thus, edge agents are distributed components associated with local elements of the ML, that is, each agent is associated with a monitoring component (or a group of them). EAs are coordinated by the Control and Coordination Agent (CCA), which is central from a logical point of view, but can be physically redundant. Each EA can use an Edge Agent Publisher or directly send the data to SMI (SCISSOR Messaging Infrastructure).

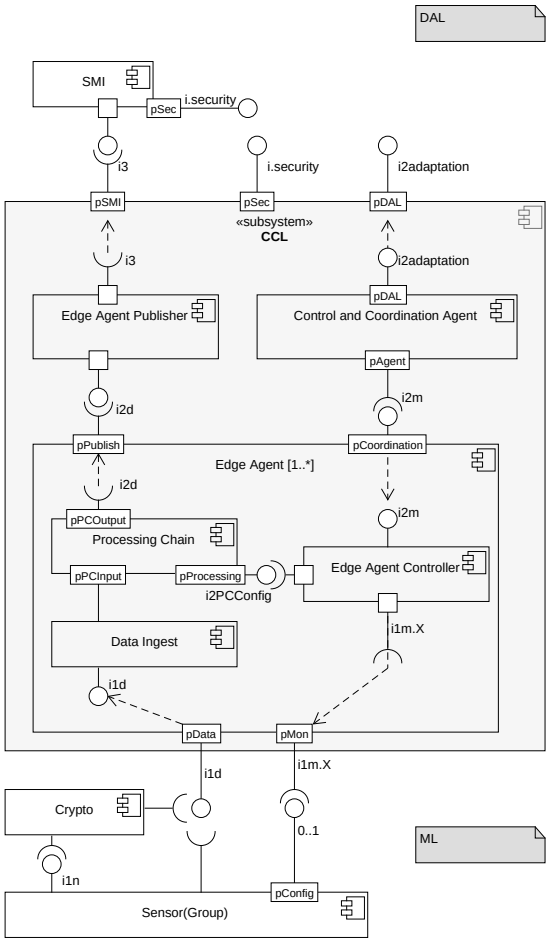


Fig. 3: Control and Coordination Layer in detail (from [22])

The use of multiple edge agents rather than a single central agent provides a high level of scalability. This means giving the system possibility to grow, increasing the amount of hardware, without the software being a limitation. In other words, new components can be attached to the system through new EAs, which are easily inserted into the CCL.

The dynamic adaptation process is driven exclusively by DAL. The control and coordination agent therefore has the function of receiving ”high-level” signals from the DAL and designating the appropriate command for the relevant edge agents. Dynamic adaptation is one of the main features of CCL, allowing the read information to be processed according to the need of the decision and analysis layer. In fact, each EA locally performs a data aggregation process and the dynamic adaptation process allows one to modify the aggregation criteria without restarting the agent.

C. Decision and Analysis Layer (DAL)

The DAL layer correlates events, detects behavioral changes, decides which ones have to be reported to the HMI and takes mitigation actions if needed [21]. It makes use of some statistical methods to create models and detect attacks.

IV. Proposed methodology

Implementing the whole system requires some resources that are currently not available and for a complete evaluation, a testbed would be necessary as well. Since the objective is to demonstrate the operation principle, we will make some simplifications in order to have a full processing chain going through all four layers.

The monitoring layer will be comprised of environment sensors, log messages and a software to read them and send the data to the upper layer. A more detailed view of the control and coordination layer is depicted in figure 3. The processing chain (figure 4) encompasses four blocks that carry out a series of operations. The Filter, in particular, performs a data aggregation task and during the course of an attack it may be reconfigured to send more or less information upwards.

Every data sent to the SMI will be available for the decision and analysis layer. To correlate the data and detect an abnormal situation (e.g. a malware deceiving the system), we propose a method based on temporal series prediction with ARMAX (auto-regressive moving average with exogenous inputs) model.

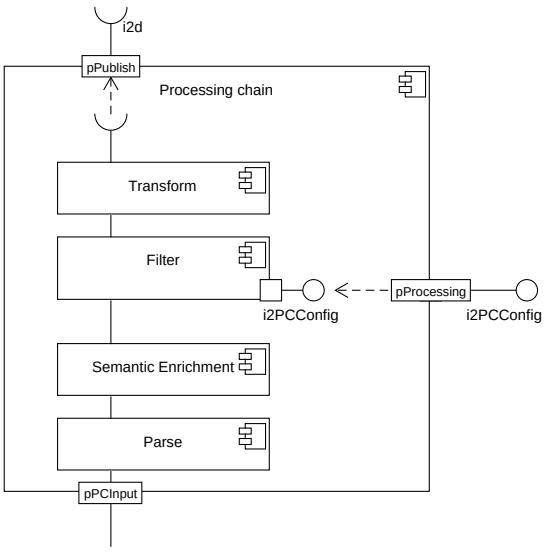


Fig. 4: Processing chain (from [22])

V. Evaluation scenario

As presented in section IV, for the evaluation test, environment sensors and log data are the chosen data sources. The simulated scenario is constructed as follows: temperature sensors and log messages report the consumed electric power. The temperature sensor is attached, for example, to an electric power board, which dissipates part of the power as heat. The correlation is direct, the more electric power is consumed, the greater energy dissipated and the warmer the board becomes.

From the transfer function relating temperature and dissipated power, we obtain the discretized transfer function (using the zero-order holder) and, thus, the difference equation. It will be then embedded in an off-the-shelf hardware, which will emulate the monitoring components.

A. Physical model

We assume a body with area A and mass m. The thermal energy dissipated by the body will, in part, warm it up and the rest will be lost to the environment. The loss is due to convection only (the black-body radiation is ignored).

$$\begin{aligned} P_d &= P_{heat} + P_{air} \\ P_d &= \frac{d}{dt}(mc(T - T_{env})) + hA(T - T_{env}) \end{aligned} \tag{1}$$

Where,

m - mass of the body [kg]
c - specific heat capacity [$\mathrm{J\,kg^{-1}\,K^{-1}}$]
h - heat transfer coefficient [$\mathrm{W\,m^{-2}\,K^{-1}}$]
A - area of the body [$\mathrm{m^2}$]

$$T_b(t) = T(t) - T_{env} \tag{2}$$

$$P_d(t) = mc\frac{d}{dt}T_b(t) + hAT_b(t) \tag{3}$$

$$\begin{aligned} H(s) &= \frac{T_b(s)}{P_d(s)} \\ &= \frac{\frac{1}{mc}}{s + \frac{hA}{mc}} \end{aligned} \tag{4}$$

Sampling with sample time T_s and applying the zero-order holder discretization,

$$\begin{aligned} H_d(z) &= (1 - z^{-1})\mathrm{Z}\left[\frac{H(s)}{s}\right] \\ H_d(z) &= \frac{1}{hA}\frac{(1 - e^{-\frac{hA}{mc}T_s})z^{-1}}{1 - e^{-\frac{hA}{mc}T_s}z^{-1}} \end{aligned} \tag{5}$$

Assuming $\alpha = \frac{1}{hA}$ and $\beta = e^{-\frac{hA}{mc}T_s}$, we obtain

$$T_b[n] - \beta T_b[n-1] = \alpha(1 - \beta)P_d[n-1] \tag{6}$$

VI. SIEM module

To have a fully functional chain, it is necessary to have a module capable of correlating the data sources and generating alerts to the HMI. In [23], the Pearson correlation coefficient was used to find the correlation between parameters of a data set and estimation was done with regression relations. In another work, a PARX (periodic auto-regressive with exogenous variables) model was employed to detect anomalies in periodic series, such as energy consumption along a day [24]. Yang et al [25] combine an auto-associative kernel regression (AAKR) with a sequential probability ratio test (SPRT) to detect denial of service (DoS) attacks.

Although the framework takes into account as many data sources as possible, we propose in the scope of this paper a method for data correlation at process level only. A regression relation would not be enough, because physical processes normally have an associated dynamics, which is unknown in principle. Moreover, such processes cannot be assumed stationary (typically time-varying mean), which is inconvenient for pure correlation measurement approaches. PARX is an interesting method, since SCADA events tend to be repetitive, so one can assume a periodic pattern.

A. ARMAX model

Based on this analysis, what we adopt is an auto-regressive moving average with exogenous inputs model, which can be used to estimate the dynamics of a system.

$$A(z)y(t) = B(z)u(t-k) + C(z)\varepsilon(t) \tag{7}$$

$$\begin{aligned} A(z) &= 1 + a_1 z^{-1} + \cdots + a_p z^{-p} \\ B(z) &= 1 + b_1 z^{-1} + \cdots + b_m z^{-m} \\ C(z) &= 1 + c_1 z^{-1} + \cdots + c_q z^{-q} \end{aligned} \tag{8}$$

Equation (7) represents the ARMAX model for a single-input single-output system. To obtain the coefficients in (8), a training data set is needed. And an algorithm, like the one in [26], can be used to train the model.

Once the estimated model is obtained, (7) is used to predict the output one step ahead $(\hat{y}_n | y_{n-1}, y_{n-2}, ..., x_n, x_{n-1}, ...)$ and the residual is calculated as $\varepsilon_n = \hat{y}_n - y_n$. We assume that the residuals ε_n are independent and identically distributed and follow a normal distribution $\mathcal{N}(0, \sigma^2)$. Those residuals are thus characterized as AWGN (Additive White Gaussian Noise) and outliers will be classified with prediction intervals.

VII. Results

Before proceeding with the results themselves, we describe the reduced architecture in figure 5. Here, the hardware used for physical process emulation is a Texas Instruments Stellaris LM4F120, acting as monitoring component. Equation (6) is embedded in the board and data (temperature and power) is sent via serial communication. The control and coordination layer ingests the raw data and applies all processing steps

according to figure 4. The result is then sent to the SMI, which is implemented with Apache Kafka, a distributed messaging system.

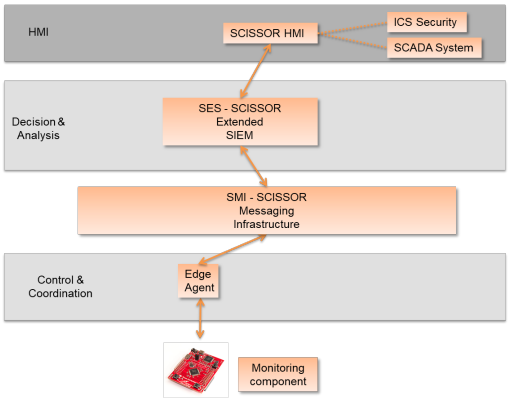
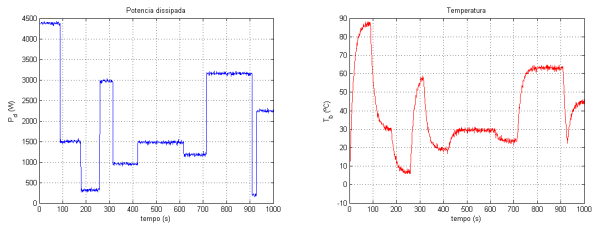


Fig. 5: Reduced architecture for evaluation mode

A. *Training*

A dataset was built to train the ARMAX model (figure 6), obtaining the coefficients in (8). The validation is depicted in figure 7.



(a) (b)

Fig. 6: Training dataset: (a) power and (b) temperature

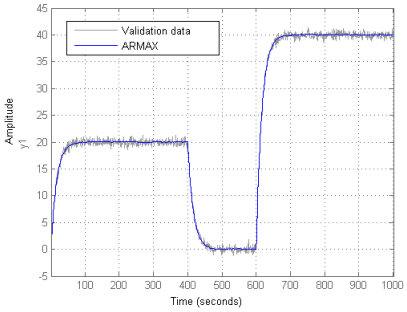


Fig. 7: Validation

B. *Full evaluation*

In this step, the complete system is in operation and the anomaly detection subsystem runs in online mode. When new information about temperature and power arrives, the SIEM module calculates the predicted temperature and compares it with the measured one. An anomaly, or a threat, is detected when an error threshold is crossed and persists for more than an established time. This threshold is calculated based on the variance of the noise σ^2 and the time based on the settling time.

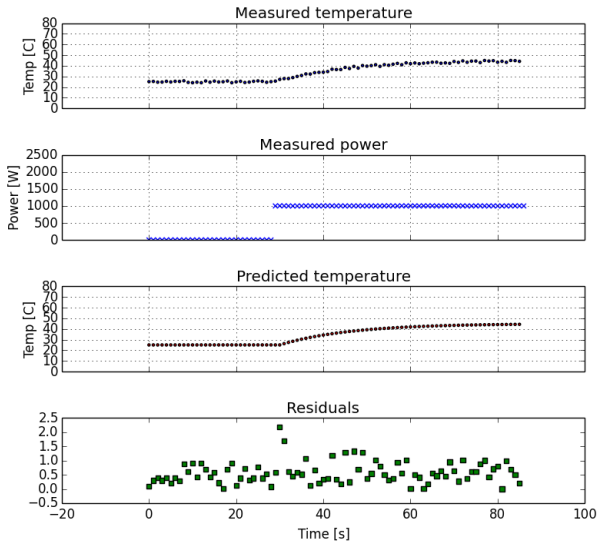


Fig. 8: Normal situation

In figure 8 a normal situation is shown, whereas in figure 9 an anomaly is occurring. Green squares represent a tolerable deviation and red triangles indicate when a potential threat is detected. The attack was forced by faking the measured power data, thus causing a divergence between the predicted and measured temperatures.

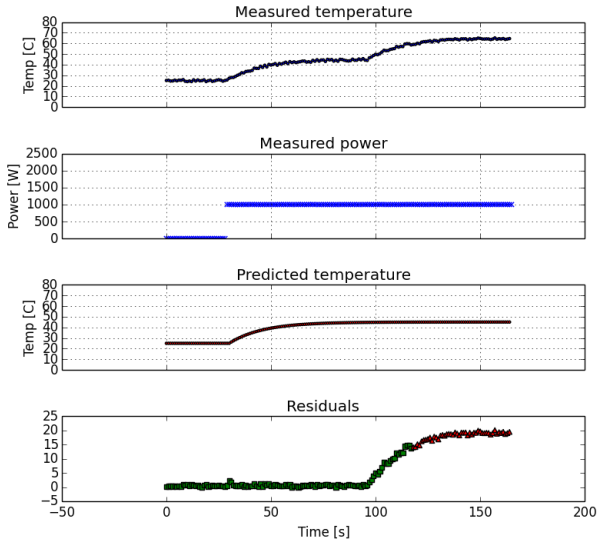


Fig. 9: Abnormal situation

VIII. Conclusion

Industrial Control Systems are related to a wide range of service, many of which being critical infrastructures, thus of high importance for society and environment. Neglecting threats to which such systems are exposed is potentially hazardous, and flaws have already been exploited by malicious adversaries, in fact. Countermeasures addressing security rising is a current topic, but there is no optimal solution. Many works propose some sort of IDS or anomaly detection system, analyzing the network and associated protocols or looking at ICS/SCADA log level.

This work presented a new layered architecture with a holistic approach, which takes advantage of the various data sources to evaluate the system state. The framework is also scalable; edge agents in the control and coordination layer are implemented in a distributed fashion and orchestrated by the DAL in collaboration with the control and coordination agent. The SCISSOR extended SIEM then uses the data gathered and processed by the CCL to detect attacks in course suspicious conditions.

Lastly, we applied this concept to a test case at process level. It is important to highlight that the chosen SIEM module can be exchanged and the layered architecture allows a modular behavior, without redesigning the other layers. Although we used a reduced scenario, the results show that the framework is functional and can be extended attaching new monitor components.

References

[1] K. Stouffer, J. Falco, and K. Kent, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security," January 2006.

[2] G. Gritsai, A. Timorin, Y. Goltsev, R. Ilin, S. Gordeychik, and A. Karpin, "Scada safety in numbers," Positive Technologies, 2012.

[3] R. I. Ogie, "Cyber security incidents on critical infrastructure and industrial networks," in *Proceedings of the 9th International Conference on Computer and Automation Engineering*, ser. ICCAE '17. New York, NY, USA: ACM, 2017, pp. 254–258.

[4] M. Krotofil and D. Gollmann, "Industrial control systems security: What is happening?" in *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, Bochum, Germany, July 2013, pp. 670–675.

[5] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, ser. ITHINGSCPSCOM '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 380–388.

[6] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, Oct. 2006.

[7] M. Korman, M. Välja, G. Björkman, M. Ekstedt, A. Vernotte, and R. Lagerström, "Analyzing the effectiveness of attack countermeasures in a scada system," in *Proceedings of the 2Nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*, ser. CPSR-SG'17. New York, NY, USA: ACM, 2017, pp. 73–78.

[8] A. Ghaleb, S. Zhioua, and A. Almulhem, "Scada-sst: a scada security testbed," in *2016 World Congress on Industrial Control Systems Security (WCICSS)*, Dec 2016, pp. 1–6.

[9] C. W. Ten, C. C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, Nov 2008.

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

[11] D. Hadžiosmanović, D. Bolzoni, and P. H. Hartel, "A log mining approach for process monitoring in scada," *International Journal of Information Security*, vol. 11, no. 4, pp. 231–251, Aug. 2012.

[12] K. Shimizu, T. Yamaguchi, T. Nakai, T. Ueda, N. Kobayashi, and B. Boyer, "A trusted approach to design a network monitor," in *Proceedings of the 5th International FME Workshop on Formal Methods in Software Engineering*, ser. FormaliSE '17. Piscataway, NJ, USA: IEEE Press, 2017, pp. 17–23.

[13] O. Yüksel, J. den Hartog, and S. Etalle, "Reading between the fields: Practical, effective intrusion detection for industrial control systems," in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, ser. SAC '16. New York, NY, USA: ACM, 2016, pp. 2063–2070.

[14] S. Mohan, S. Bak, E. Betti, H. Yun, L. Sha, and M. Caccamo, "S3a: Secure system simplex architecture for enhanced security and robustness of cyber-physical systems," in *Proceedings of the 2Nd ACM International Conference on High Confidence Networked Systems*, ser. HiCoNS '13. New York, NY, USA: ACM, 2013, pp. 65–74.

[15] J. Nivethan and M. Papa, "A scada intrusion detection framework that incorporates process semantics," in *Proceedings of the 11th Annual Cyber and Information Security Research Conference*, ser. CISRC '16. New York, NY, USA: ACM, 2016, pp. 6:1–6:5.

[16] R. L. Krutz, *Securing SCADA Systems*. Indianapolis: Wiley, 2005.

[17] D. McMillen, "Security attacks on industrial control systems," 2015, research report.

[18] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. I. Sidorov, and A. A. Timorin, "Industrial control systems vulnerabilities statistics," 2015, research report.

[19] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," 2011, research report.

[20] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, March 2013.

[21] S. Salsano, "SCISSOR Architecture Specification," CNIT, Parma, Italy, Tech. Rep., 2015.

[22] C. Tavernier, C. Brandauer, and P. Dorfinger, "Revision of Control Framework: Design and Implementation," Salzburg Research Forschungsgesellschaft, Salzburg, Austria, Tech. Rep., 2016.

[23] A. Hassanzadeh and B. Sadeghiyan, "A data correlation method for anomaly detection systems using regression relations," in *2009 First International Conference on Future Information Networks*. Washington, DC, USA: IEEE Computer Society, Oct 2009, pp. 242–248.

[24] X. Liu and P. Nielsen, "Regression-based online anomaly detection for smart grid data," p. 11, June 2016.

[25] D. Yang, A. Usynin, and J. Hines, "Anomaly-based intrusion detection for scada systems," 07 2008.

[26] H. Spliid, "A fast estimation method for the vector autoregressive moving average model with exogenous variables," *Journal of the American Statistical Association*, vol. 78, no. 384, pp. 843–849, 1983.