ENHANCING SAFETY AND SECURITY OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEM BY EVENT AGGREGATION

Robert Altschaffel[1], Fan Zhang[2], Jianghai Li[3], Jonas Hielscher[1], Tamas Holczer[4], Wen Si[3], and Kevin Lamshöft[1]
[1]Working Group Mulitmedia and Security, Otto von Guericke University, Magdeburg, Germany,
firstname.lastname@iti.cs.uni-magdeburg.de
[2]Department of Nuclear Engineering, University of Tennessee, Knoxville, TN, USA, fan@utk.edu
[3]Institute of Nuclear and New Energy Technology , Tsinghua University, Beijing, China,
lijianghai@tsinghua.edu.cn, siw17@mails.tsinghua.edu.cn
[4]Laboratory of Cryptography and System Security, Budapest University of Technology and Economics,
holczer@crysys.hu

ABSTRACT

Nuclear power plants (NPPs) are implementing or transitioning to digital instrumentation and control (I&C) systems to control underlying physical processes. Such systems present an attack surface of obvious interest to various subsets of potential attackers and hence lead to a relevance of cybersecurity in a nuclear context. This prompts the need for measures aimed at detecting anomalous behavior or unwanted events in the I&C systems. This paper performs a survey on existing approaches to detect such behavior. This survey covers different perspectives and a broad range of different anomalous or unwanted behavior in the physical process and all aspects of the digital I&C systems. The perspective benefits from the inclusion of experts from the field of NPP cybersecurity, automation engineering and IT security. This interdisciplinary perspective allows for the identification of different sets of relevant data and events which might contribute to the understanding of an abnormal or unwanted situation (malfunction or a cyber-attack). This paper discusses how this data should be collected, how it can be aggregated and in which way it can enhance the safety and security of digital I&C systems.

Key Words: NPP Cybersecurity, I&C Security, SIEM, IDS, Anomaly Detection

1. INTRODUCTION

The implementation and transition of Nuclear power plants (NPPs) to digital instrumentation and control (I&C) systems for the control of underlying physical processes greatly enhances the means to measure and control the complex physical processes and also supports the operator by including mechanisms to detect anomalous behavior of the underlying physical process. However, such I&C systems itself present an attack surface of obvious interest to various subsets of potential attackers and hence lead to a relevance of cybersecurity in a nuclear context. This prompts the need for measures aimed at detecting anomalous behavior or unwanted events in the I&C systems.

Currently, various means to detect anomalous or unwanted events in the underlying physical process as well as in the I&C systems itself are available, deployed or currently researched. Examples for this include unusual network connections or values outside of the intended operational range. Understanding a potential relationship between such events is relevant for the identification of cyber-attacks or faults within the digital I&C systems. Hence an integration of information provided by various means of detecting anomalies in the computerized control process as well as in the physical process might be able to increase the resilience of NPP digital I&C systems and thereby increasing safety of the underlying processes and security of the control systems.

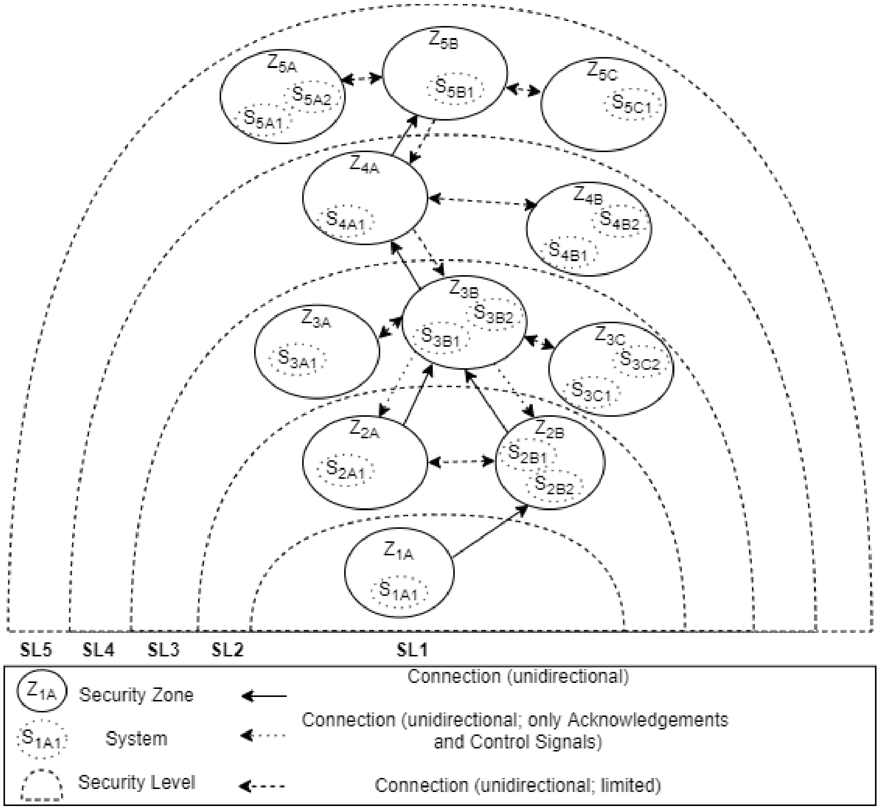

Figure 1. Security Levels and Security Zones based on [1]. Intra-Zone communication is omitted.

This paper performs a survey of detection approaches for anomalies and attacks in the context of NPPs. This survey combines different view points from relevant fields including cybersecurity in the NPP domain, automation engineering and IT-security. Differences in focus, wording, priority and understanding of critical components are overcome in order to accumulate the specific knowledge and to discuss a reference architecture for event aggregation and all the events relevant for the detection of anomalous and unwanted behaviour (including cyber attacks) in the NPP domain. These differences show that the exchange of interdisciplinary knowledge is necessary to advance cybersecurity in NPP contexts. The remainder of this paper is structured as follows: Section 2 presents the general structure of digital I&C systems. Section 3 provides a survey of multiple approaches to detect abnormal or unwanted behavior. Section 4 discusses an overall framework for event aggregation in the context of NPP. Section 5 discusses and summarizes the findings.

2. GENERAL STRUCTURE OF DIGITAL I&C

This section provides an overview of the general structure of digital I&C in NPPs. This overview is aligned with the guidelines for the *Defensive Computer Security Architecture* (DCSA) provided by the IAEA in [1]. These guidelines group the various components of the digital I&C and the IT systems present within an NPP environment into five different *Security Levels* and various *Security Zones*. The Security Levels are defined in [1] as follows:

- **Security Level 1 (SL1)**: Systems vital to the facility (e.g. physical emergency protection)
- **Security Level 2 (SL2)**: Operational control systems which require high security
- **Security Level 3 (SL3)**: Supervision systems not required for operations

- **Security Level 4 (SL4)**: Technical data management systems (e.g. used for maintenance)
- **Security Level 5 (SL5)**: Business systems

In general, digital I&C systems are found in **SL1**, **SL2** and **SL3**. **SL4** and **SL5** mostly cover traditional IT systems. The information flows between the Security Levels are strongly restricted due to security policies. **SL1** allows only for strictly unidirectional communication to **SL2**. **SL2** is restricted to outward communication to **SL3** with the allowance for necessary acknowledgement messages and a set of well-defined control signals. Between **SL3** and **SL4** only specific and limited communication is allowed. Between **SL4** and **SL5** uncontrolled network traffic is restricted by security gateways.

Security Zones are physical or logical groupings of systems with the same need for protection. Hence, all systems within a Security Zone are part of the same Security Level. A Security Zone represents a trusted environment. Although less clearly defined as with the borders between different Security Levels, Security Zones should contain decoupling mechanisms from other Security Zones within the same Security Levels. Hence, they should be bordered by security gateways which prevent uncontrolled network traffic. The overall architecture and the permitted communication is shown in Figure 1.

The overall architecture usually contains *Historians* which record information about the physical process. A *Process historian* is usually located on **SL3** in order to provide information about the trends of the physical process to the operators. A *Plant historian* is usually located on **SL4** in order to record and store historical data about the physical process.

3. SURVEY ON APPROACHES TO DETECT ABNORMAL OR UNWANTED BEHAVIOR

This section provides an overview on the approaches and data sources to detect abnormal or unwanted behavior either through the use of digital I&C system or within the NPPs. This is followed by survey on the means to detected abnormal or unwanted behavior within the digital I&C system which might be caused by cyber-attacks. Thereby, the surveyed approaches come from different domains.

3.1. Detection of Abnormal or Unwanted Behavior of the Physical Process

This section provides an overview on the detection of abnormal or unwanted behavior of the physical process. This data is referred to as *process data* during the course of this paper.

Figure 2 provides an overview on the general logic of anomaly detection using process data, (including the detection of cyber-attacks). Expected physical values, such as temperature, flow rate, and pressure, are predicted by the use of machine learning approaches and/or statistic models. These predictions are based on input from real sensor measurements - either the current measurements or previous measurements. The differences between the real sensor measurements and the predicted values are referred to as *residuals*. Fault detection techniques, such as simple thresholds and cumulative sum (CUSUM), are applied to these residuals to generate alarms to indicate the deviation from the normal operation. This and familar approaches have been used to detect cyber-attacks based on process data:

- Goh et al. [2], proposed an unsupervised Long Short Term Memory Recurrent Neural Network (LSTM-RNN) to predict the sensor values and utilized cumulative sum (CUSUM) method to the residuals to detect cyber-attack. The data set utilized to evaluate the effectiveness of the approach was collected under seven-day normal operation and four-day operation with cyber-attacks from a large scale Secure Water Treatment Testbed (SWaT), a six-stage raw water dispute testbed for cybersecurity research built by Singapore University of Technology and Design [3].

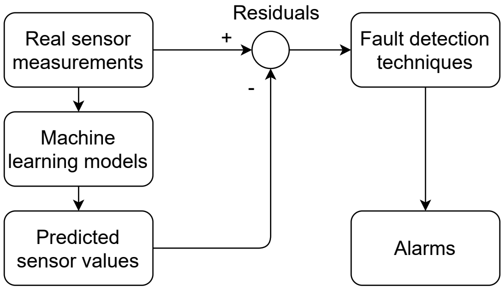

Figure 2. General logic of anomaly detection using process data.

- Gawand et al. [4], utilized least square approximation to detect cyber-attacks. A model of a four-tank control was built using state equations as a virtual testbed for this research. The results showed that the detection approach was effective on two numerically simulated cyber-attacks.

- Kiss et al. [5], developed a Gaussian mixture cluster model to detect the simulated attacks by modifying the data from the Tennessee-Eastman chemical process model (see [6]).

- Nader and Honeine [7,8], utilized real data from a SCADA gas pipeline tested and the water treatment plant to investigate the effectiveness of the anomaly detection of two one-class classification models, kernel principal component analysis (KPCA) and support vector data description (SVDD), for cyber-attack detection. The abnormal transient in the data was regarded as the cyber-attacks. The results showed that KPCA has better detection than SVDD.

- Li et al. [9], proposed to use dynamic principal component analysis (PCA) to model the correlations of sensors under normal operational condition and a chi-squared detector to perform the fault detection of the residuals. Eggers [10], utilized independent component analysis (ICA) and PCA with both static and moving window to detect simultaneous physical- and cyber-attacks simulated by modifying the real normal process data from an NPP.

- Zhang et al. [11] [12], developed several unsupervised models cyber-attack detection using process data, including auto-associative kernel regression (AAKR), auto-associative support vector regression (AASVR) model, auto-associative principal component regression (AAPCR), and auto-associative ensemble regression. A real-time ICS testbed that simulates a two-loop nuclear thermal hydraulic system was built with a SCADA system to generate both, process- and cyber-data [13]. An hardware-in-the-loop (HIL) testbed were built based on a nuclear system simulator and a Programmable Logic Controller (PLC) [14] for cybersecurity research. Zhang et al. [15], also proposed a localized attack detection model using process data to enhance the cybersecurity for key equipment in nuclear facilities.

- Gazdag et al. [16], predicated the state of Cyber Physical Systems (CPS) to detect anomalies with statistical models, where the detection was integrated into the well known Bro IDS.

3.2. Detection of abnormal or unwanted Network traffic

Zhang et al. [11] developed supervised models, including decision tree, k-nearest neighbors (KNN), bootstrap aggregating (Bagging) and random forest, to detect DoS and MITM attacks using network traffic data generated from the ICS testbed [13]. Zhang et al. [17], also utilized an AAKR model to detect MITM attack using network flow data, collected by Argus [18] on the ICS testbed [13]. In [19] Lamshöft et al.

show how Information Hiding based attacks might render common Network Intrusion Detection Systems (NIDS) found in conventional IT-systems insufficient and require for custom detection methods.

3.3. Detection of abnormal behavior of Controllers

The modern I&C system integrates multiple controllers, connected by a communication network into the physical plant process through sensors and actuators. The detection of anomalies occurred in components and parameters of plant dynamic, as well as in the sensors and in the actuators has been studied in the research branch of fault detection and diagnosis (FDD) [20]. The controllers and the communication network were assumed to be normal in the literature of FDD. However, it is not the case in the presence of cybersecurity. Several research have been done in the anomaly detection of controllers, such as PLCs [21, 22].

3.4. Correlation Engine/Decision Engines

Analysing separate security events is cumbersome and not really efficient. Correlating the events is a tedious work which should be automated. To solve this natural need, correlation engines are used. A correlation engine can find the relations between different events automatically, and can help the operator to focus only on the events which require attention. The correlation of events in an NPP is really challenging as events from the traditional IT network and events from the physical process must also be considered.

- Surveys on Security Information and Event Management Systems (SIEM) and their correlation engines can be found in [23, 24].

- Most of the correlations engines are manually configured to find the related events. Some preliminary work on automatic correlation learning can be found in [25] where the correlation engine automatically learns and produces correlation rules based on the context for different types of multi-step attacks using genetic programming.

- Bou-Harb et al. [26], created a *CPS Threat-Detector* that performs signature based anomaly detection by combining data from malware reports and a Honeypot with data from physical processes.

- Altschaffel et al. [27], introduced the idea of a *Nuclear SIEM*, a monitoring system that correlates IT-data (network data) and OT-data (information about the physical processes). Altschaffel [28] also describes the use of *C0f Fingerprinting Tool* to detect anomalous behaviour in the network communication of vehicular communication networks and states and furthermore that this approach could be adapted to the use with ICS due to the similarity of these domains. This approach is based on heuristic information about the prevalence of certain message types during the network and is able to detect unusual communication behavior quickly without the need to analyse the payload of the communication in detail.

4. CONSIDERATIONS FOR AN OVERALL FRAMEWORK

In this section the ideas and key concepts from the survey and the considerations for and from the domains are aggregated into a reference architecture. To develop such the following questions need to be answered.These questions touch on various design considerations and interact with each other. In this light, it is necessary to keep in mind the overall goal of enhancing the (cyber-)security of the digital I&C without endangering the safety. The primary questions are **PQ1**: which data has to be collected and **PQ2**: where it has to be collected. From this, some secondary questions arise: **SQ1**: how the data has to be collected, **SQ2**: how the data should be stored and **SQ3**: who has access to the data (and the results of the aggregation).

The fundamental question **PQ1** affects all the other questions. Since the secondary questions greatly influence **PQ2** they are answered before **PQ2** is discussed.

Table I. Data relevant for the event aggregation system

Type of data	Physical domain **PD**	Cyber domain **CD**	Network domain **ND**	External domain **ED**
Normative Data	Model of the physical process, alarm points for certain values, schematics of the physical process	Configuration of the PLC (including IP-Addresses), schematics of the PLC structure	MAC-Whitelist, IP-Whitelist, Network plans	Maintenance schedules, Vacation plans, Access lists
Live Data	Physical values	PLC Data (Uptimes, Cycle Times, Resource Usage, IP-Addresses, User access), PLC Logs, User Access Logs	Netflow data [17], Network captures, Firewall Logs, SNMP, Switch Logs	Persons currently in the facility
Abnormalities	LSTM-RNN [2], Key equipment data [15]	HIDS alerts, PLC alerts [21, 22]	Firewall alerts, NIDS alerts [11]	PPS alerts, IT SIEM alerts
Aggregations	Events aggregated over different domains (e.g. an abnormal state of the physical process following a PPS alert) [23, 24, 26, 27]			

PQ1: Which events should be collected? The detection methods discussed in section 3 rely on a broad range of data. Based on these data, abnormal behavior within a given subsystem is detected. This can be considered as the generation of an event reporting an abnormality within a given subsystem. The occurrence of such events can be correlated with events in different subsystems resulting in a correlated event.

This fundamental understanding can be used to describe four different kinds of data stored within such an event aggregation system: (1) *Normative data* that is available independently from the current state of the system and represents the desired overall state (e.g. models for the physical process, security policies for the allowed communication). (2) Basic data points (*Live data*), which represents the live state of the system but for themselves do not indicate abnormalities. (3) Events generated from the detection of abnormal behavior within a given subsystem (*abnormalities*). (4) events aggregated from different subsystems (*aggregations*).

These three kinds of data can originate from three different domains present within the digitized I&C system. One domain addresses the physical process (*physical domain* - **PD**) and covers data about the state of the physical process. The other domains cover the state of the computing units (*cyber domain* - **CD**) and the network respectively (*network domain* - **ND**). Additional input comes from sources outside of the digital I&C - this source is referred to as *external domain* - **ED**). This includes information from the IT (**SL4** and **SL5**) as well as from the physical protection system. The information gathered from the IT is usually also based on the **CD** and the **ND** within the IT-section. This approach allows for a systematic identification of data as well as a classification of the approaches presented in section 3 as shown in Table I.

SQ1: How should the data be collected? The data should be collected without endangering the safety and security of the overall system. As such, the collection of the data should be handled in a passive manner. This means that the data transferred to the aggregation system is strictly unidirectional. The different data domains require different methods to conduct this data collection. In the case of the **PD** this could be implemented by an additional unidirectional connection to the sensors. In the case of **ND**, the network traffic can be captured by a passive network probe. In **CB** passive access is more difficult since PLC data is usually not broadcast. However, the data collected by a localized secure measures could be duplicated and collected. It is essential to keep in mind where the data is collected. For example, the measurement of the temperature at given sensors can be obtained in different ways. At first, the reading of the sensors could be duplicated directly at the source, it could be obtained from the PLC attached to this sensor and using the measurement for a computation or from the values reported the HMI, MCR or historians. In general, obtaining a value directly from the source grants a higher degree of authenticity. Since a difference between the reported values at these different locations might in itself point towards some abnormal behavior, collecting multiple instances representing the same value might be useful.

SQ2: How should the data be stored? The data should be collected in a reliable manner to ensure the integrity and authenticity. This is comparable to the requirements placed by IT-Forensics (see [29]) and can therefore rely on established procedures from this domain. Cryptographic measures, like Keyed-Hash Message Authentication Code, can be used to prevent an undetected modification of the stored data. This data should also include reliable timestamps - ideally those provided by the data collection point (sensor, network probe or specific security measure) as well as those provided by the event aggregation system itself. Beyond this, it is necessary to store information about how a certain piece of data was obtained. As discussed in **Q3**, physical measurements are presented in various instances across the entire digital I&C system.

In addition, the data collected in such an event aggregation system is highly critical and hence should be protected from unauthorized access. Confidentiality is the primary security concern in this case. Hence, the data should be encrypted with access only granted on a restricted basis.

SQ3: Who has access to the data (and the results of the aggregation)? The data collected within the event aggregation system is critical in terms of cyber security while being complex to interpret. This restricts the number of people that should have access to this data and those that benefit from having access.

The interpretation of the aggregated data requires a set of skills combining an understanding of the different domains where the data originate. While there might be automated approaches for correlating events (as stated in section 3) the interpretation of such lays in the hands of domain experts and their ability to correlate events of different domains to a single cause.

The operators in the Main Control Room (MCR) are experts with regards to **PD**. However, a deep understanding of **CD** and **ND** is also necessary in order to utilize collected and aggregated data. However, it also goes beyond the field of a network security operator (who focuses on **ND**). This role might be filled by a new, unique position with an overview in all the respective fields - a dedicated OT cyber security operator.

Making the aggregated information solely available to such a position would also minimize exposure of all the collected critical information. In this case, the dedicated operator would be in close contact with the operators of the MCR and might be situated in the same physical space as these operators to facilitate a quick reaction in case of a cyber-attack.

PQ2: Where should the collected data be stored? The collected data should be stored where it is accessible to those that can benefit from it and inaccessible to potential attackers. As discussed before, access should be granted to dedicated OT cyber security operator working in close contact with the MCR.

This seems to suggest a positioning on **SL3** in the MCR. Another potential position would be on **SL4** in conjunction with the plant historian. **SL1** and **SL2** are excluded due to the strict security policies preventing any form of data aggregation. Another approach would be the inclusion of an event aggregation systems with no physical bidirectional communication connections towards any of the various security levels. This isolated system would only passively receive information and store them. Physically this systems could be located in the MCR and be supervised by the OT cyber security operator.

Table II. Pros and Cons for the placement of the aggregation on different security levels

Placement	Pro	Con
MCR on **SL3**	Direct access to process historian and control signals (**PD**), Easy access to **ND** between **SL2** and **SL3**, **CD** can be propagated from **SL2** without violating security policies, information is accessible to MCR operators	MCR has direct access to aggregated data, **ED** must be passed down
SL4	Direct access to plant historian (**PD**), Direct access to **ED**	**ND** and CD must be propagated from **SL2** and **SL3**, MCR has no direct access to aggregated data
Isolated system	Direct unidirectional access to process historian and control signals (**PD**), Easy unidirectional access to **ND** between **SL2** and **SL3** and to **CD** from **SL2** information is accessible to MCR operators	**ED** must be passed down

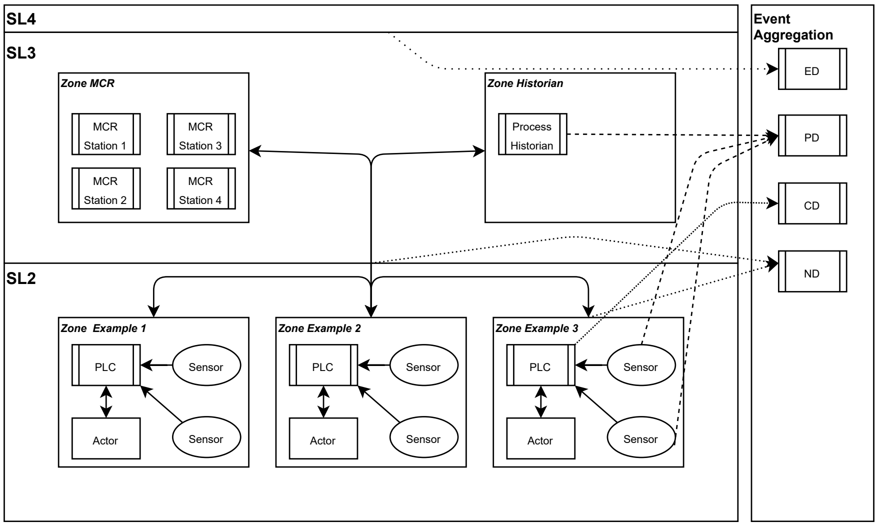

Figure 3. Suggested placement of the event aggregation system with exemplary connections for data collection from the different domains.

These options are compared in Table II with a draft of the architecture of such an isolated event aggregation systems visualized in 3. The isolated system supports the integrity of the digitized I&C system as well as the confidentiality of the collected and aggregated data.

5. CONCLUSION

This work presents a system survey on the means and methods to detect abnormal and unwanted events by the use and within digitized I&C systems in the nuclear domain. This data is put in a framework to better facilitate event aggregation between these events from different sources, domains and of different classes available within digitized I&C systems. To facilitate this, previous approaches from the network-, cyber-, physical- and other domains were summarized and compared. The key findings were accumulated into a reference architecture that aims at detecting security and safety threats that would usually stay undetected in case only single sources were considered. This architecture can be used as a foundation for further considerations that aim with data correlation between different domains. The results also show that it is important that experts from the different domains come together and use a common understanding of security threats, domains and classes of events.

The complex understanding necessary to ensure cyber security with OT environments in the nuclear context prompts the need for dedicated OT cyber security operators or the inclusion of specific cyber security courses within the training of NPP operators.

ACKNOWLEDGMENTS

The work from Robert Altschaffel in sections 1,2 and 4 was partly funded by the German Federal Ministry for Economic Affairs and Energy within the project SMARTTEST2 (Grant No.: 1501600B). Jonas Hielschers contribution is based on his Bachelor Thesis providing input for section 3.4 and 4. Fan Zhang would like to thank the Lloyd's Register Foundation and the International Joint Research Center for the Safety of Nuclear Energy for partial funding.

REFERENCES

[1] "Computer Security Techniques for Nuclear Facilities," IAEA (2011).

[2] J. GOH, S. ADEPU, M. TAN, and Z. S. LEE, "Anomaly detection in cyber physical systems using recurrent neural networks," *Proc. 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, p. 140–145, IEEE, 2017.

[3] J. GOH, S. ADEPU, K. N. JUNEJO, and A. MATHUR, "A dataset to support research in the design of secure water treatment systems," *Proc. International Conference on Critical Information Infrastructures Security*, p. 88–99, Springer, 2016.

[4] H. L. GAWAND, A. BHATTACHARJEE, and K. ROY, "Securing a cyber physical system in nuclear power plants using least square approximation and computational geometric approach," *Nuclear Engineering and Technology*, **49**, *3*, 484 (2017).

[5] I. KISS, B. GENGE, and P. HALLER, "A clustering-based approach to detect cyber attacks in process control systems," *Proc. 2015 IEEE 13th international conference on industrial informatics (INDIN)*, p. 142–148, IEEE, 2015.

[6] A. BATHELT, N. L. RICKER, and M. JELALI, "Revision of the tennessee eastman process model," *IFAC-PapersOnLine*, **48**, *8*, 309 (2015).

[7] P. NADER, P. HONEINE, and P. BEAUSEROY, "L^p -norms in one-class classification for intrusion detection in SCADA systems," *IEEE Transactions on Industrial Informatics*, **10**, *4*, 2308 (2014).

[8] P. NADER, P. HONEINE, and P. BEAUSEROY, "Intrusion detection in SCADA systems using one-class classification," *Proc. 21st European Signal Processing Conference*, p. 1–5, IEEE, 2013.

[9] J. LI and X. HUANG, "Cyber attack detection of I&C systems in NPPS based on physical process data," *Proc. 2016 24th International Conference on Nuclear Engineering*, p. V002T07A011–V002T07A011, American Society of Mechanical Engineers, 2016.

[10] S. L. EGGERS, *Adapting Anomaly Detection Techniques For Online Intrusiondetection In Nuclear Facilities*, PhD thesis, University of Florida, 2018.

[11] F. ZHANG, H. A. D. E. KODITUWAKKU, W. HINES, and J. B. COBLE, "Multi-Layer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System and Process Data," *IEEE Transactions on Industrial Informatics*, **5**, *7*, 4362 (2019).

[12] F. ZHANG, J. W. HINES, and J. B. COBLE, "A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities," *Nuclear Technology*, **206**, *7*, 939 (2020).

[13] F. ZHANG, J. W. HINES, and J. COBLE, “Industrial control system testbed for cybersecurity research with industrial process data,” *Proc. International Congress on Advances in Nuclear Power Plants (ICAPP 2018), Charlotte, NC, USA, April 8-11, 2018*, 2018.

[14] F. ZHANG, *Cybersecurity Solutions for Industrial Control Systems and Key Equipment*, PhD thesis, University of Tennessee, Knoxville, 2019.

[15] F. ZHANG and J. B. COBLE, “Robust localized cyber-attack detection for key equipment in nuclear power plants,” *Progress in Nuclear Energy*, **128**, 103446 (2020).

[16] G. M. ANDRáS GAZDAG, TAMAS HOLCZER, “Intrusion detection in Cyber Physical Systems Based on Process Modelling,” *Proc. Proceedings of 16th European Conference on Cyber Warfare & Security*, Academic conferences, 2016.

[17] F. ZHANG, J. COBLE, and J. W. HINES, “DATA-DRIVEN MODEL APPLICATION FOR ATTACK DETECTION OF SCADA SYSTEM,” *Proc. 11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2019), Orlando, FL, USA, February*, 2019.

[18] L. QOSIENT, “Argus,” *see: http://www. qosient. com/argus/index. htm* (2004).

[19] K. LAMSHöFT et al., “Novel Challenges for Anomaly Detection in I&C Networks: Strategic Preparation for the Advent of Information Hiding based Attacks,” *atw - International Journal for Nuclear Power*, **65**, 504 (2020).

[20] A. MOUZAKITIS, “Classification of Fault Diagnosis Methods for Control Systems,” *Measurement and Control*, **46**, 303 (2013).

[21] K. YAU, K. P. CHOW, S. M. YIU, and C. F. CHAN, “Detecting anomalous behavior of PLC using semi-supervised machine learning,” *Proc. 2017 IEEE Conference on Communications and Network Security (CNS)*, p. 580–585, 2017.

[22] Y.-J. XIAO, W.-Y. XU, Z. JIA, Z.-R. MA, and D.-L. QI, “NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers,” *Frontiers of Information Technology & Electronic Engineering*, **18**, 519 (2017).

[23] S. S. SEKHARAN and K. KANDASAMY, “Profiling SIEM tools and correlation engines for security analytics,” *Proc. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, p. 717–721, IEEE, 2017.

[24] L. ROSA, P. ALVES, T. CRUZ, P. SIMÕES, and E. MONTEIRO, “A comparative study of correlation engines for security event management,” *Proc. Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security*, p. 277, 2015.

[25] G. SUAREZ-TANGIL, E. PALOMAR, A. RIBAGORDA, and I. SANZ, “Providing SIEM systems with self-adaptation,” *Information Fusion*, **21**, 145 (2015).

[26] E. BOU-HARB et al., “Cyber Meets Control: A Novel Federated Approach for Resilient CPS Leveraging Real Cyber Threat Intelligence,” *IEEE Communications Magazine*, **55**, *5*, 198 (2017).

[27] R. ALTSCHAFFEL, T. HOLCZER, C. NEAL, and M. HILDEBRANDT., “The Nuclear SIEM,” *Third International Conference on Nuclear Security: Sustaining and Strengthen-ing Efforts (ICONS 2020)* (2020).

[28] R. ALTSCHAFFEL, *Computer forensics in cyber-physical systems : applying existing forensic knowledge and procedures from classical IT to automation and automotive*, PhD thesis, Otto von Guericke University Magdeburg, 2020.

[29] R. ALTSCHAFFEL, M. HILDEBRANDT, S. KILTZ, and J. DITTMANN, “Digital Forensics in Industrial Control Systems,” *Proc. Computer Safety, Reliability, and Security*, p. 128–136, Cham, 2019, Springer International Publishing.