Nuclear Engineering and Technology 52 (2020) 2687–2698

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Review Article

A new perspective towards the development of robust data-driven intrusion detection for industrial control systems

Abiodun Ayodeji [a], Yong-kuo Liu [a, b, *], Nan Chao [a], Li-qun Yang [a]

[a] Fundamental Science on Nuclear Safety and Simulation Technology Laboratory Harbin Engineering University, Harbin, 150001, China
[b] State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment Shenzhen, Guangdong, 518172, China

ARTICLE INFO

Article history:
Received 16 January 2020
Received in revised form
18 March 2020
Accepted 11 May 2020
Available online 12 May 2020

Keywords:
Cybersecurity
Intrusion detection system
Nuclear power plant
Pattern recognition

ABSTRACT

Most of the machine learning-based intrusion detection tools developed for Industrial Control Systems (ICS) are trained on network packet captures, and they rely on monitoring network layer traffic alone for intrusion detection. This approach produces weak intrusion detection systems, as ICS cyber-attacks have a real and significant impact on the process variables. A limited number of researchers consider integrating process measurements. However, in complex systems, process variable changes could result from different combinations of abnormal occurrences. This paper examines recent advances in intrusion detection algorithms, their limitations, challenges and the status of their application in critical infrastructures. We also introduce the discussion on the similarities and conflicts observed in the development of machine learning tools and techniques for fault diagnosis and cybersecurity in the protection of complex systems and the need to establish a clear difference between them. As a case study, we discuss special characteristics in nuclear power control systems and the factors that constraint the direct integration of security algorithms. Moreover, we discuss data reliability issues and present references and direct URL to recent open-source data repositories to aid researchers in developing data-driven ICS intrusion detection systems.

1. Introduction

Recently, digital devices are being introduced into industrial control consoles to replace aging and obsolete analog control systems and to enhance the decision-making process. In cyber-physical systems (CPS), the introduction of digital systems has produced a network of safety components with programmable logic controllers (PLCs), which provide information useful for control optimization and lifespan extension. The shared compatibility of digital systems has led to the proliferation of IT devices in monitoring CPS network data traffic. However, utilizing shared devices exposed the traditional opacity common in legacy CPS control, as the vulnerabilities associated with these digital systems have been inherited by the safety systems and these cyber vulnerabilities partly account for the recent surge in cyber-attacks. Moreover, cyber assaults on process control and monitoring systems could lead to a significant control failure such as spurious valve position change, pump control loss, sudden feed water loss and the failure of safety-critical components as demonstrated by the Stuxnet worm attack [1], Davis-Besse nuclear plant attack [2] and California system operator attack [3].

Recent developments in industrial data acquisition systems have spurred a renewed interest in the utilization of data-driven approaches to curb the rise of industrial cyber-attacks. Some machine learning-based intrusion detection systems (IDS) monitor traffic and dataflow at the operating system (host intrusion detection system - HIDS) or at the network level (network intrusion detection system - NIDS) to detect attacks targeted at the host or the network. For the HIDS development, the host-based packet captures (PCAP) are preprocessed and applied in training the data-driven model, while the NIDS utilizes the network layer information for model development. However, the implementation of both the host-based and network-based solutions in complex industrial systems are limited because cyber-attacks have a real and significant impact on the process variables or the physical system. Conversely, some process-based intrusion detection systems (PIDS) have also been developed using process measurements alone. This approach has the same weakness as NIDS because analyzing the

* Corresponding author. Fundamental Science on Nuclear Safety and Simulation Technology Laboratory Harbin Engineering University, Harbin, 150001, China.
E-mail address: lyk08@126.com (Y.-k. Liu).

https://doi.org/10.1016/j.net.2020.05.012

process change in isolation would not provide a significant clue regarding the causal path.

In an attempt to improve the capability of existing IDS for sophisticated attack detection in cyber-physical systems, some researchers have integrated both host/network traffic and process layer information to develop a robust detection system. A major drawback to adopting this approach is that in complex industrial systems, process variable change could result from normal operating transients, incipient system fault, component degradation, sensor drift, cyber-attacks, or the combination of a number of these occurrences. The existing accounts fail to resolve the differences between the process changes resulting from different initiating events. This limitation results in an intrusion detection system with a high false alarm rate, and the high false alarm rate has rendered many of the proposed solutions un-implementable.

The primary goal of this paper is to introduce the discussion on the similarities, conflicts, and limitations of the tools commonly used by fault diagnosis and cybersecurity practitioners—two areas that are having an increasing connection with the advancements in machine learning (ML) and pattern recognition algorithms. This paper is based on the following observations:

1. Similar datasets or signatures are being used to develop pattern classification tools for detecting cyber-attacks (PIDS) and to diagnose faults in cyber-physical systems. We believe these tasks are fundamentally different, and it is imperative to establish the differences and domain-specific requirements necessary for the effective implementation of the tools.
2. Many reported cyber-attacks carried out on cyber-physical systems usually appear as system malfunction or fault injection, and there is a need to build a system with the capability to recognize and recover from both incidents without complicating the already complex system, and with no hindrance to other safety-related functions.
3. Attackers are adaptive and dynamic. Tools developed to detect adaptive attacks should be adaptive, as the attacker could exploit the vulnerabilities discovered in the tools and undermine their effectiveness. Extending pattern classification theory and design methods to security settings without considering the adversarial influence is ineffective. Data can be manipulated by attackers to undermine IDS functionality and attacks can be directed at the IDS itself.
4. Pattern recognition systems commonly used in adversarial environments without a detailed threat assessment may result in classification systems that exhibit vulnerabilities whose exploitation may severely affect their performance and consequently limit their practical utility.

These observations have severe implications for research that utilizes system datasets for abnormal occurrence detection. To extensively discuss the main thesis of this paper, we first present a brief description and characteristics of the industrial SCADA system and preliminaries on the existing ML algorithm in section 2. Then in section 3, we enumerate different data domains and techniques used in the development of ML-based intrusion detection systems for ICS with emphasis on the issues and limitations of the resulting algorithms. As a case study, the nuclear plant control system, its operating states and common system signatures that are similar to the once obtainable during random system fault and cyber-attacks are discussed. In section 4, we describe IDS evaluation methods and discuss the reliability of the dataset available to researchers, which is critical in the development of a functional ML-based intrusion detection algorithm. Section 5 is a discussion on proposed techniques and recommendations for the development of an effective abnormal occurrence detection system applicable to complex industrial controllers.

2. Preliminaries

2.1. SCADA system

Supervisory Control and Data Acquisition (SCADA) has been consistently defined to include embedded systems, sensors and actuators used in monitoring and control of critical industrial and national infrastructures such as smart grid, transportation networks, and power generating plants. Supervision, control and data acquisition functions of SCADA are achieved by some computer-based applications and networked devices. Automatic and user-defined real-time monitoring and control of process measurements are performed through remote terminal units (RTU), intelligent field-programmable devices, and their networks.

Successfully implementing defense against cyber-attacks on critical SCADA infrastructure depends on understanding the vulnerabilities attributed to the specific SCADA system. The SCADA operating environment is characterized by special input voltage, different mounting options, utilization of proprietary operating system without security hardening, infrequent patch update, and the use of special protocols with limited computing capabilities [4]. In modern.

ICS where controllability and integrity are prioritized, these characteristics have security implications with potentially catastrophic consequences [5]. There have been efforts to quantitatively evaluate and share information on discovered vulnerabilities in information technology systems [6]. Government-owned repository of security-related software flaws and vulnerabilities with data on common vulnerabilities and exposures (CVE), and the associated impact analysis tools such as the common vulnerability scoring system (CVSS) and common weakness enumeration (CWE) [7,8] are existing attempts to document and quantify security risks. Also, in SCADA systems, there have been attempts to share known vulnerabilities and SCADA network test tools used to secure against cyber exploits [9]. However, for privacy and security considerations, there are no known publicly available repositories for common vulnerabilities in industrial-scale SCADA systems.

The inadequacy in utilizing the conventional ICT security technologies for SCADA systems and the inherent differences between the characteristics of the information technology security approach and that of SCADA systems and components have been demonstrated [10]. The strong real-time constraints and requirements for the domain-specific cyber-security approach for critical infrastructures have also been explained [11,12]. To address the security gaps observed in industrial control systems, some innovative approaches to critical digital assets security have been presented. A one-way and dual-path data diode that allows data to flow in a single predetermined direction is being used to defend against the cyber threat in some US nuclear installations. The architectural design uses diodes to provide a form of physical separation between the operation of technology comprising digital instrumentation and control, and the conventional information technology space usually referred to as the business space in nuclear power facilities. Data diode has been praised for its simple set up and installation procedure, as well as its low maintenance cost [13]. However, it is inadequate, as complete isolation of critical cyber assets, single destination gateway, installation cost, software support, and insider threat/human reliability issues still exist [13].

2.2. ML tools for SCADA IDS

Machine learning algorithms and other artificial intelligence

models are being used in different fields to solve different problems. Clustering algorithms such as Naïve Bayes, Random Forest, NB Tree, support vector machine, neural networks, and an ensemble of soft computing algorithms have been used to diagnose complex system faults [14,15]. K-means recursive clustering [16,17], Hidden Markov Model [18], Adaboost [19], fuzzy-based inference system and its variants [20,21] have also been previously utilized for access control in a metro system [22], and for embedded intrusion protection systems [23]. To build better classifiers, these algorithms are often ensemble homogenously or heterogeneously, with specific decision rules. To address security issues in SCADA systems, some researchers have also utilized the real-time functionality of machine learning algorithms to detect malicious network traffic in SCADA systems [16,24] and for other intrusions and anomaly detection purposes [25,26]. Different SCADA intrusion and anomaly detection techniques have also been combined into a single hybrid system with decision rules [12,27]. Basically, the development of ML algorithms for ICS security application involves the following steps:

I. Identifying and obtaining threat signatures that represent the intrusion to be detected (for signature-based, misuse detection approach) or obtaining normal traffic features (for anomaly-based approach).
II. Preprocessing and segmentation of the data into training, testing, and validation set.
III. Identifying the confidence level required, and tuning the hyper-parameters accordingly.
IV. Evaluating the performance of the algorithm on the representative data as input to the trained model and comparing the output within the range of the confidence interval selected.

Variation in the implementation is observed in the spread of the data used and the training techniques employed. Depending on the sophistication of the algorithm, the training method, and the level of automation involved, data preprocessing procedure could vary from manual data sorting and partitioning to online adaptive training with data obtained from field devices. Various heuristic refinement and innovative training optimization techniques are being utilized to enhance ML algorithms classification, clustering, or predictive accuracy. Optimization techniques include iterative online training with heterogeneous data [19], data scaling and normalization [28], data dimensionality reduction with statistical models and cross-validated data processing to improve learning speed and detection time [29,30] and integrating multiple learning techniques to reduce overfitting. Meta-heuristics and hyper-parameter selection approach also vary for different algorithms. The selection methods for neural networks' hidden layer transfer function, layer number, optimal hidden neuron size, and output layer activation function are discussed in Ref. [28]. Kernel-based support vector machine heuristic selection and optimization for various classification and regression problems and the application-dependent confidence level requirement for each algorithm are also discussed in Ref. [30,31]. Further tutorials on machine learning or data mining methods for intrusion detection are presented in Ref. [32,33].

3. Similarities and conflicts in ICS fault monitoring and cybersecurity

3.1. Common techniques for developing data-driven IDS

Most of the available security solutions and protective techniques against cyber-attacks in critical systems are focused on extending traditional IDS networking needs and requirements that generally match attack signatures using a signature-based IDS or detect network anomalies with machine learning techniques [34]. In the development of signature-based IDS, attack patterns are aggregated and processed to train the algorithm. Each traffic data is labeled (supervised training) or clustered (unsupervised/semi-supervised training) according to a specific pattern generated during the attack. Anomaly-based systems utilize normal traffic data for training and testing, and the anomaly is detected when there are exceptional changes or deviation from known traffic. Robust anomaly detection algorithms rely heavily on specific domain protocols and legitimate characteristics of the target system for efficient performance. Signature-based IDS rely on historical attack signatures on specific systems for intrusion detection. This is a kind of hypothesize-and−match technique where signatures of known attacks are used to train the algorithm. However, signature-based IDS cannot detect novel attacks, as it is impractical to acquire signatures of all types of attacks in a single dataset. Also, the second-order chaotic nature of exploits such as stealthy or spy attacks makes novel attack prediction and simulation difficult. Fig. 1 shows a detailed flow chart for the development of industrial IDS.

To support the argument in this section, we define a few terminologies that could be ambiguous. We define the terms based on their uses in engineering maintenance and complex system security.

1. System fault: A spontaneous or slowly-developing, non-malicious defects that cause detectable process deviation from the recognized system's behavior. Such system faults include component degradation, sensor drift, fouling or crud formation on pipes, heat exchanger ruptures, etc.
2. Cyber-attacks: Hostile, malicious invasion of controls systems and components with the potential to affect the availability, integrity or confidentiality of the safety functions performed by the control systems. It can also be a result of malicious misuse, insider exploits resulting in anomaly behavior that impacts the control system, networks or the process.

There are attacks aimed to exploit the vulnerabilities in network-level based compatible field devices (e.g. DOS, DDOS, etc) and there are some attacks aimed to exploit the SCADA process controller itself (e.g. MITM, false sequential logic attack, etc). Several IDS developers rely on data traffic from the network or host domain alone.

Others utilize data from the physical process while some integrate the information from different domains. The following subsections describe each IDS development, its implementation challenges, and functional limitations.

3.2. Host/network domain-based IDS models

Network traffic features contain SCADA communication patterns and information on the device such as the address, the packet source, the packet, and function code length, etc. SCADA communication protocols can be specifically targeted by corruption, interception, or tampering attacks. These can potentially lead to a loss of confidentiality, visibility, or device connectivity, and also provide support to implement process-aware attacks, thus compromising safety and security.

The contemporary intrusion detection algorithms on information technology assets are based on network traffic classifiers built with IP network flows. Recently, an extension of the detection system based on network behavior or host monitoring has been utilized for intrusion detection in industrial control systems. This technique uses anomaly-based or signature-based misuse

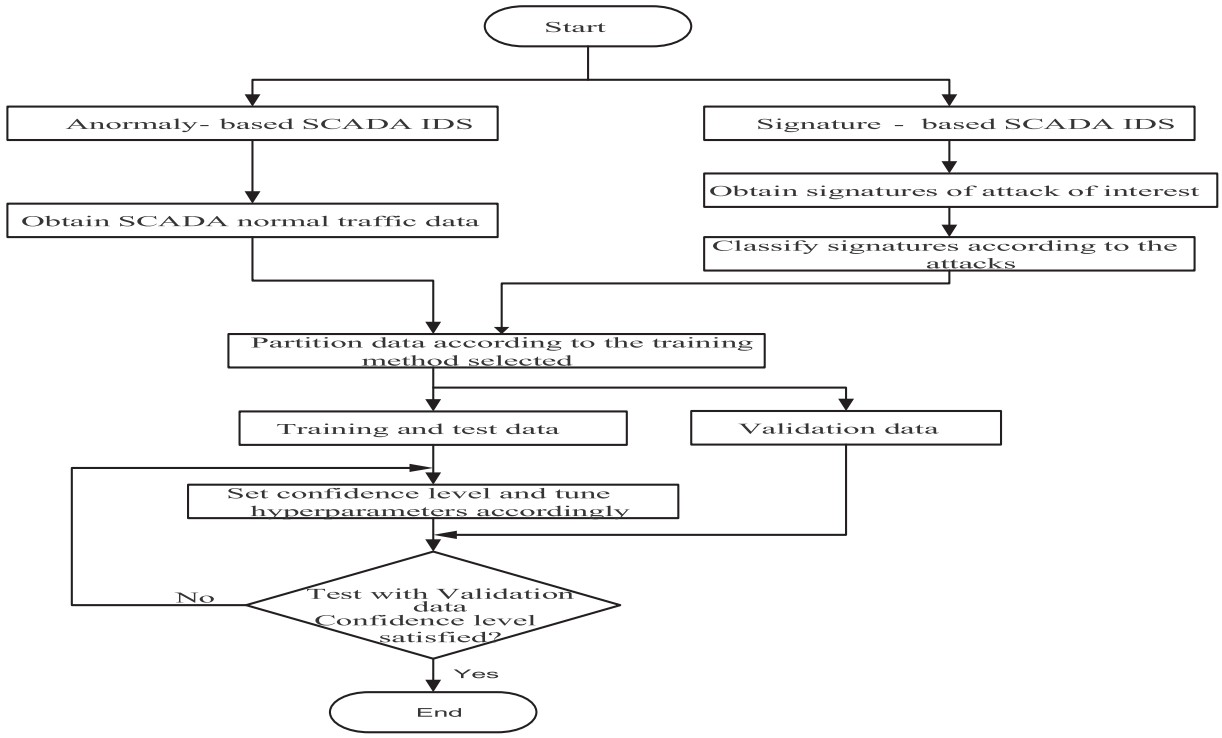

Fig. 1. Flow chart for the development of industrial IDS.

detection models to detect system intrusion. As a signature-based model, this approach involves creating a database that contains all the signatures of the known payload attributes and single packet-based attacks on SCADA protocols and using this database in the development of the IDS. However, apart from the paucity of the SCADA-specific training dataset, the signature-based approach is ineffective in detecting novel attacks because updating attack signatures is hard. Also, some zero-day, advanced persistent attacks common to ICS have signatures that are not particularly known. Considering these limitations to the development of signature-based IDS, researchers now utilize an anomaly detection algorithm.

As an anomaly-based model, the approach involves inspection of signals that specifies normal traffic, and building a model that can identify the normal traffic pattern and flag abnormal usage. This algorithm is built with normal system traffic data, and any deviation from the normal operation is flagged as an anomaly. Fuzzy inference systems and artificial neural networks were applied in Refs. [35,36] to increase the security awareness of embedded cyber sensors using network-level data. Network scanning tools, Nmap and Nessus, were utilized to create abnormal network behavior in an experimental control system testbed. The detection systems were constructed based on the feature stream in the network traffic packets. Anomaly-based IDS is relatively easy to build as the data requirement is almost homogenous, and it is convenient for application where the acquisition of attack signature is difficult. It has a relatively simple design as it only processes a single data stream from the network feed and does not require attack signatures. However, the model is limited in real-world applications because it cannot identify and localize attacks. Moreover, port registration, the legality of interception, and critical operational requirements for network packet inspection and port-based analysis are other issues to yet be resolved [37]. A more important limitation of this approach in critical infrastructures is that process measurement is essential in detecting attacks. Control and safety is the fundamental ICS function which makes it an attractive target for sophisticated attackers. This is partly because of the technical sophistication and resources that are available for threat actors interested in such a facility. Hence, the historical behavior of the physical process is critical to detect ICS cybersecurity incidence, and the process parameters are the most effective indicators of the historical and current state of the system and control functions.

3.3. Process measurement-based model for IDS

The discovery of attackers with partial or total control of the sensor or actuator has led to the proposal of several intrusion detection schemes for ICS using data collected from physical sensors. To achieve the maximum return on the attack, most SCADA penetration targets critical control devices such as sensors and actuators. The exploit of these devices results in a significant impact on the process measurements and the physical system. To develop robust IDS, many researchers consider the application of process variables. The logic considers attack scenarios such as false data injection and deceptive man-in-the-middle (MITM) attacks that could mask the real process state or present spurious parameter measurement to manipulate the control response. For instance, an attacker with access to process configuration could launch an attack to modify process set-point and trigger undesirable system response.

Li et al. [38] demonstrated the utility of process parameters in detecting cyber intrusion by investigating a false sequential logic attack on the SCADA system using process-level parameters. Analysis of the physical effect of the attack on a simplified pump-valve control system shows the possibility of serious process disruption and equipment damage. Anomalies in a water supply control system were detected using signal variations from a control system to train and evaluate KNN, SVM and Random Forest algorithms [39]. In this approach, process parameter deviations and process variables non-conformity to natural behavior are used as indicators of the anomaly. Data representing features expected in

normal operations of the system is derived first. This dataset is used to develop the anomaly detection algorithm. In the implementation phase, the algorithm monitors the real-time operation of the system and compares the real-time features with the features derived from normal operations. In some applications, a dynamic threshold is set to flag the comparison result that is beyond a certain level of deviation from the normal features. An intrusion is detected when a flag is generated. This is usually based on the possibility that an attacker may pass a deceptive measurement in place of real measurements, and manipulate control response, an instance of data injection or false operation attack.

Behavioral modeling tools such as the autoregressive model is being used to monitor for changes to high-value variables that would normally stay constant [40]. A state-based intrusion detection system for MODBUS-DNP3 network traffic is presented in Ref. [41]. Complex attacks are detected by considering the transitioning of the system from known steady, secure state to significant process deviation that results in the critical system failure. The state change information, process control knowledge and internal representation of the SCADA system are utilized for intrusion detection. Also, detecting the advanced persistent threat in the SCADA system is possible through process monitoring. However, the attractiveness of this method is beclouded by the fact that there are many initiating events for process change. As previously stated, observed deviation could be a result of normal operating transients, incipient system fault, component degradation, sensor drift, cyber-attacks or the combination of a number of these occurrences.

Incidentally, the real-time pattern attributes in the process measurements also make it suitable for diagnosing system or component faults. This attribute has been utilized to build independent ML models for fault diagnostic purposes using only process measurement. For instance, process deviation has been used to diagnose the reactor coolant system and component faults using neural networks [28], and support vector machine [29,30]. Evolutionary algorithms and optimized statistical models have been used to diagnose leakages in industrial steam generators [30,31]. Moreover, some of the reported cyber-attacks seek to compromise ICS by first defeating the safety measures put in place. This method of attack could be easily mistaken for a random fault. Diagnosing the breach and identifying the root cause takes time and expertise. For instance, the changes in a process variable for offset or geometric attack that involves constant or time-dependent addition of spurious values to the sensor or actuator output, and the variable trend noticed for an incipient leakage in heat exchanger pipes or reactor pump seal leakage may be difficult to differentiate. The similarity in trend and signature may obscure the causal path and eventually result in - at best − a false positive, or - worst case - a more serious misdiagnosis resulting in safety breach and other consequences of successful advanced persistent attacks. Fig. 2 shows the possible causal path for the observed process change in complex industrial systems.

An attempt to distinguish between different anomalies by analyzing the anomaly behavior based on the instrument output data has been proposed by Jie et al. [42]. They argued that instrument output beyond a fixed band, transfer function similarities in the input-output relationship between two adjacent switch devices and logical relationships in state values can be used to distinguished between system failure, DoS attack, and false data injection. However, they also utilized process level measurement alone for the analysis. Moreover, the simple system analyzed to evaluate the method does not represent the dynamics observed in complex systems as demonstrated in section 3.4. Also, setting a fixed threshold for a system with such dynamics is not viable. Moreover, a similar method is prominent in fault identification and isolation research work, especially for fault isolation and localization involving sensor drifts and dropped packets.

The limitation in this model further explains the simplistic approach and the reluctance in the real-world implementation of some of the researched intrusion detection systems. Some researchers [43,44] recognized the inherent weakness in the PID system and considered integrating process-level information with the network traffic data for robust intrusion detection.

3.4. Multi-domain data mining technique for IDS development

To address the issues identified with homogenous data-driven intrusion detection systems, several researchers developed IDS algorithms built on both host/network traffic data as well as process-level knowledge to strengthened ICS security. Morris and Gao [45] utilized network traffic information and state-based payload content features such as sensor measurements and distributed control state to detect anomaly in a SCADA system. Zhang et al. [44], utilized heterogeneous data derived from the simulation of five attacks on a private ICS testbed. They compared the classification performance of K-means, random forest and decision tree on the data from the testbed. However, this approach also suffers from the limitation of the process level intrusion detection. A much more systematic approach would identify how various initiating events (shown in Fig. 2.) interact to change the process variables. The implementation of such a model in a real-world system is bound to result in high false alarm rates. Table 1 summarizes the available IDS techniques and decision engines utilized.

3.5. Case study: process measurements change initiating events in the nuclear power plant

In complex systems such as nuclear power plants, there are some operating transients and load changes that characterize the normal operation of the plant. To ensure the balance of plant, a typical nuclear power plant utilizes many distributed control and safety systems designed to ensure safe operation and - in case of an accident - safe shut down and cooling of the reactor core. In normal operation, the neutron population and fission rate are being controlled by several systems such as control rod and chemical shim. In a typical PWR, minor reactivity or power adjustment is done with the aid of the chemical and volume control system (.i.e. boric acid). Also, based on the turbine-generator configuration for the reactor, changes in the power demand from the grid could necessitate a corresponding change in the power supply from the reactor. All these changes introduce a unique dynamic into the control of the nuclear power plant which needs to be integrated for the robust development of IDS suitable for detecting attacks in such systems. Fig. 3 shows a simplified representation of the nuclear plant control system.

In Fig. 3, Layer 1 is the physical level where the sensor and actuators are utilized to control the physical system. The second layer (Layer 2) is the distributed controllers responsible for implementing automated control based on the current state of the component being monitored. The controllers utilize the automatic feedback response from the current process measurement output to set the next stage of the process. In industrial control systems, this function is carried out by devices such as programmable logic controllers (PLCs). These controllers have internal memory with the capability to process control logic for the attached component and to relay the measurement to the operator through the process control network. Layer 3 is the process control network, where the detection, control, and monitoring functions are usually performed. Control and communication protocols such as Modbus, DNP3, etc are used to ensure effective flow of control and safety signals. Beyond the automated functions in Layer 2, additional safety and

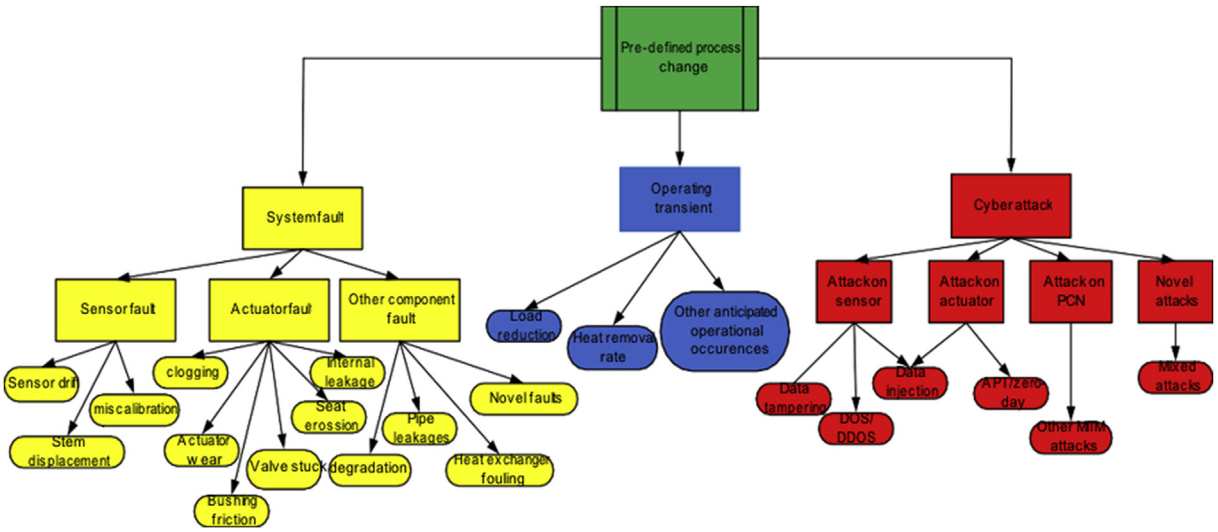

Fig. 2. Potential initiating events for the observed changes in industrial process parameters.

Table 1
Commonly used technique for developing ICS intrusion detection systems, data type and the decision engine utilized.

IDS Technique	Training Dataset source	Data type	Decision engine	References
Network traffic/host-based	Testbed[a]	[b]Synthetic	OCSVM; K-mean clustering	[16,17]
	KDD	Real	ANN, Neighborhood outlier Factor	[46]
	NSL-KDD	Synthetic	GA-SVM; FNN	[14,20]
			1-class SVM	[47]
			DNN	[48,49]
	UNS-NB15	Synthetic	DNN	[48]
	DARPA 1998	Real	ANN, SVM, MARS	[15]
	ADFA-WD	Synthetic	ANN, SVM, HMM, ELM, STIDE	[50]
	ADFA-LD	Synthetic	KNN, HMM, STIDE, Naïve Bayes, k-means, SVM SMO,	[51,52]
	Testbed	Synthetic	SVM; KNN, Decision tree; Random forest	[53]
Process variable-based	Testbed	Synthetic	Association rules	[42]
	Suez water distribution dataset	Real	One-class SVM	[54]
Integrated approach(Network traffic and process variables	***CIPC-MSU water dataset	Synthetic	SVM, ANN etc.	[22,55,56],
	ORNL dataset	Synthetic	EM clustering	[57]
			KNN; NB, RF	[58]
	iTrust –SwaT Dataset	Real data	ANN; DNN	[59,60]
	Testbed	Real data	KNN, decision tree, random Forest	[44]

[a] Testbeds include the scaled-down version of the SCADA system that controls a real physical process or uses a hardware-in-the-loop (HIL) simulation of the physical process.
[b] Synthesized data include those generated from SCADA mimics, workbenches, and sanitized data. Acronyms: ELM = Extreme learning machine; HMM= Hidden Markov Model EM = expectation-maximization STIDE: Sequence Time-Delay Embedding; DNN = Deep neural network; FNN = fuzzy neural network; MARS = Multivariate Adaptive Regression Splines.

control signals are routed through the process control network. Layer 4 is the supervisory control and data acquisition layer with a direct connection to the process control network. Here, the process measurements are stored in a data historian. The dataset in this historian are analyzed for fault diagnosis and maintenance purposes. This layer also contains systems such as the control consoles, workstations, servers, network equipment and systems with a human-machine interface where operators can monitor and control the physical process.

A key aspect of this ICS security is the validity of the data values sent from programmable logic controllers to the HMI. An attacker could gain remote access to Level 2 sensors and actuators modify their software or their environment or intercept the transmission. With this access, attackers could launch coordinated attacks on the physical system through the process being controlled. An attacker who can manipulate the data values can mount attacks with severe consequences. Access to layer 2 devices could also empower the attacker to trick the human operator by sending spurious measurements [61]. Another major consideration is the process measurement dynamics introduced when complex ICS system undergoes routine maintenance or part replacement. These dynamics also affect the process measurement trends used in the development of some intrusion detection systems. In constructing robust IDS applicable to the complex system utilized in the control of a nuclear plant, it is pertinent to consider the nuances introduced by the control of the plant, as well as the causal path of other

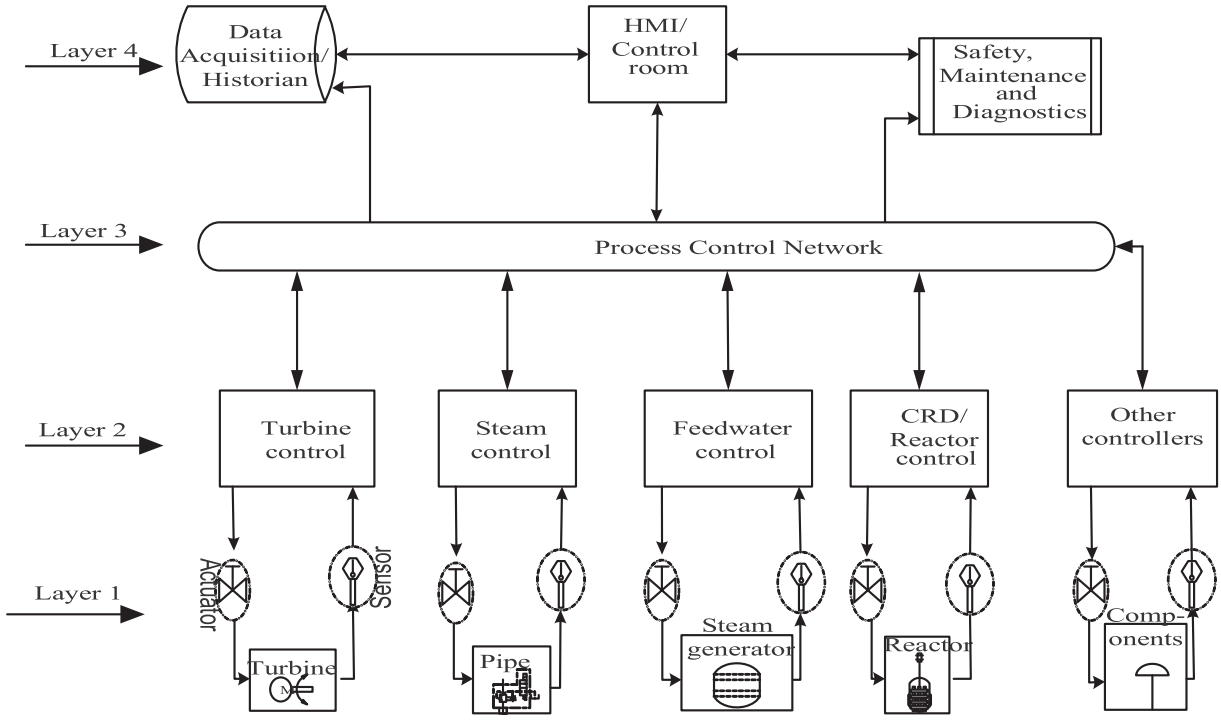

Fig. 3. A simplified process control system for a typical nuclear power plant.

possible abnormal occurrences.

To further elaborate on the similarities in some stated attack and incipient fault, consider the development of a state-aware intrusion detection system for stealthy man-in-the-middle attacks against ICS field-bus water tank level control system discussed in Ref. [62]. The study depicts a false data injection attack where the attacker gains root access to sensor measurement and actuator command (level 2 as illustrated in Fig. 2) and forces a decrease in water level in a simulated industrial water tank. The attacker slowly changes the sensor reading of the tank level using a small constant increment, trying to remain undetected [62]. Also, the study designs a detection mechanism that relies on the residual which is the difference between sensor measurement for the water level and its estimated value. There are obvious similarities in the signatures generated in this instance and many diagnostic approaches for incipient, slowly-developing faults that also rely on process level change [31] and residual generation for system fault detection.

Moreover, modeling and simulating the transients explained above is not a trivial task. Researchers utilize several computer codes to simulate process control and acquire process parameter deviations. However, the outputs of the codes are estimates with limited applications. Similar constraints are present in NIDS development. Simulating attacks that represent real-world exploit to retrieve signatory data, or to evaluate ML model performance is difficult. Hence, most researchers rely on publicly-sourced data to train, test, and evaluate the intrusion detection system. In the next section, we examine the composition of public data repositories and their reliability for developing ICS intrusion detection systems.

4. IDS data sources and data reliability

The key element that determines the optimum performance of any data-driven model is the quality of the data used in its development. Effective application of ML approach to intrusion detection requires significant training data. Also, proper implementation and reliability of the IDS depend on the sources and credibility of the dataset. Datasets that contain normal and malicious traffic is scarce and developers rely on abstracted simulation or synthesized network traffic in publicly available data repositories to train the ML algorithms. This is even more pronounced for critical ICSs, where obtaining historical data of attacks is difficult. Commonly used public database for NIDS is presented in Table 2. A prominent source is the data presented by NSL-KDD, an improvement on KDD 99 dataset. KDD and its variant, NSL-KDD dataset has been applied to develop IDS models such as artificial neural network and neighborhood outlier factor [46], one-class support vector machine [16,47] and fuzzy neural network [14,20]. The Center for Applied Internet Data Analysis (CAIDA) and other repositories that captures full or truncated local network packets including some background traffic, useful for IDS researchers are also listed in Table 2. Australian defense force academy windows dataset (ADFA-WD) and Australian defense force academy Linux dataset (ADFA-LD) are some of the later adaptation for UNIX-based operating systems which houses signatures of some contemporary cyber threats sourced from exploiting vulnerabilities in virtual kernel-based hosts. ADFA-LD and ADFA WD dataset utilized system call distribution pattern and the number of traces contained in each class as the metric for training ID algorithms, based on previous research on the accuracy of system calls traces for decision engines. Data traces are collected and utilized for the training and validation of IDS decision engines. The dataset structure and raw trace count for both Linux and Windows OS are as shown in Table 3. References to other datasets and repositories of packet capture for network-based intrusion detection systems are listed in Ref. [63].

Furthermore, categories of attack modeled to generate each dataset are different, as it is impractical to model all possible attacks in a single experiment. Table 4 contains the attacks simulated to generate the dataset for KDD, UNSW-NB15, and NSL-KDD datasets and the number of instances for each attack. The distribution of the data depends on the attack simulated and the domain

Table 2
Open source data set for NIDS security research.

Data source	Description	Reference
ISCXIDS201 2	Repository of real traces from real network traffic collected and developed through research at the ISCX	[64]
CAIDA	Internet traffic data and links to varieties of other collections	[65]
UNIBS-2009	Anonymized traces collected by U. Brescia Ground Truth (GT) software suite.	[66]
UMass Trace Repository	A collection of network and multimedia traces for IDS analysis	[67]
NFNSM data	Repository of IDS-related packet capture traces for network security monitoring and open source PCAP repositories by the Network Forensic and Network Security Monitoring	[68]
CSE-CIC-ID S 2018	captured network traffic and system logs for seven different attack scenarios on 420 machines and 30 servers, along with 80 features extracted from the captured traffic	[69]
IES dataset	Network traffic for TCP/UDP packets	[70]
UNM dataset	Collection of synthetic and live traces for system calls executed by active processes	[71]
CICIDS2017	Repository of network traffic analysis of benign and common attacks with source and destination IPs, source and destination ports, protocols and attacks.	[72]
KDD-UCI	A collection of datasets from UCI Center for Machine Learning and Intelligent Systems	[73,74]
NLS-KDD	A repository of sanitized KDD-related data	[75]
CIPC-MSU water dataset	Data repository of the Critical Infrastructure Protection Center at the Mississippi State University (MSU)	[45,56],
ADFA	Australian defense force academy dataset for UNIX-based operating systems which houses signatures of some contemporary cyber threats sourced from exploiting vulnerabilities in virtual kernel-based hosts	[50]
UNSW-NB15	Australian Centre for Cyber Security (ACCS) generated packet captures of a hybrid of real modern normal activities and synthetic contemporary attack behaviors.	[76,77]

Table 3
Attack category and instances in KDD, UNSW-NB15 and NSL-KDD datasets.

Attack category	Number of instances (Training + Test)		
	KDD	UNSW-NB15	NLS-KDD
Remote to local(R2L	1126	–	77,054
Probing/Exploits	4107	44,525	14,077
Denial of service(DoS)	391458	16,353	53,385
User to root(U2R)	52	–	252
Analysis	–	2,677	–
Backdoor	–	2,329	–
Fuzzers	–	24,246	–
Generic	–	58,871	–
Reconnaissance	–	13,987	–
Shellcode	–	1,511	–
Worms	–	174	

considered. Commonly used dataset for SCADA and ICS intrusion detection is presented in Table 5. Some of the repositories contain data from legacy systems commonly found in industrial control systems, while some combine the process measurements and packet capture from advanced SCADA systems.

Data acquisition cost, privacy, and data source reliability considerations have restricted most of the proposed ML-based IDS to fixed, simplified parametric algorithms. Data paucity results in constrained, weak algorithm, which poorly fit the data and cannot process complex problems. Data inadequacy also results in biases that are reflected in the performance of IDS systems [78]. Security considerations inform the privacy imposed on ICS data and common vulnerabilities discovered in SCADA systems. Hence, most research and commercial intrusion detection solutions project the successes recorded in developing and testing the tool on other platforms. Unfortunately, the dataset collected for a certain system configuration is not a sufficient representation for all other application and the full range of attack surface presented by different hosts. For instance, as demonstrated in section 3.5, the SCADA architecture in NPP and device connection varies from other industrial control systems because of imposed special safety requirements. Consequently, the data generated from such a connection would be unique. Hence, application-specific traffic would have to be collected for a comprehensive evaluation of the performance of the tools meant for such systems. Moreover, in the openly available data examined, there is no consideration for the heterogeneous data requirement discussed in section 3.3. Where the data is heterogeneous, it fails to consider other causalities presented in Fig. 2, hence they are not representative of the real-world complexity observed in industrial control systems. Also, for security reasons, a number of the publicly available packet traces are released in anonymized form, while some did not specify the payload.

Data benchmarking is another challenge, because threat actors and attack dataset evolve rapidly, making it difficult to rely on dated data. Moreover, attack paths and malicious behavior considered for each data set vary, as comprehensively capturing all possible malicious intents and attacks for all ICS configurations is not feasible. Besides, some of the testing and evaluation technique is subjective. Many models are tested and evaluated on randomly sampled data from the training set, resulting in reports of impressive accuracy in theory, but high false positives on real-world systems. This also makes an independent evaluation of SCADA IDS a difficult task. Biased models are some of the results from deficient, highly synthetic, non-representative data, skewed and redundant records present in the publicly available dataset [75,78]. Existing datasets face other reliability challenges. One is the fact that some repositories have an unlabeled dataset, and labeling them for application purposes is difficult. Considering the size of data needed for developing a robust intrusion detection model, some repositories contain an insignificant amount of dataset or incomplete payload.

The value and ultimate reliability of a particular dataset depend on the acquisition framework and application expertise. Hence, we did not attempt to compare the performance of different datasets in this work. Nevertheless, research work towards verifying KDD and NSL-KDD as benchmark data set shows that the data set lacks modern low footprint attack style, the normal traffic data is outdated and there is a mismatch in the attack types, resulting in different distribution for training and test dataset [77]. Currently, there is no known effort to quantify the effect of synthetic data on the real-world performance of the algorithm. Moreover, proclivity for any of the datasets and user's preference decisions are unclear,

Table 4
ICS network packet captures (PCAP) and process measurement data repository.

Data source	Description	Reference
ORNL dataset	Oak Ridge National Laboratory's repository of measurements related to normal, disturbance, control and cyber-attack behaviors for electric transmission systems, gas pipeline, and energy management system.	[79]
ASL ICS traffic repository	Repository of intercepted attack packets on ICS CTF with Modbus/TCP and Siemens S7comm traffic by Artisan Safety Lab	[80]
iTrust-SWaT repository	Collection of network traffic and process measurement data on a fully operational scaled-down water treatment plant.	[81]
4SICS Repositories	ICS dataset and industrial network equipment for hands-on testing.	[82]
DigitalBond PCAPS	DigitalBond S4x15 ICS Village CTF PCAPs	[83]
CSET-2016 dataset	Labeled packet captures for both malicious and non-malicious SCADA Modbus traffic and accompanying CSV files, generated from a SCADA sandbox.	[84]
ICS PCAP repositories	Compilation of ICS PCAP files indexed by the protocol for ICS/SCADA utilities and protocols	[85]
UCCT-ICS PCAP	Cybersecurity PCAP repository by University of Coimbra cybersecurity team	[53]
2000 DARPA Dataset	Defense Advanced Research Projects Agency DARPA intrusion detection evaluation on LLDOS and WindowsNT	[86]
LBNL/ICS Packet Traces	A set of ICS packet header traces from October 2004 through January 2005	[87]

Table 5
Threat models and their evaluation metric.

Threat model/Attacks analyzed	Evaluation metrics	References
DoS, MITM, NetScan	Classification accuracy; detection speed	[16]
NSL-KDD attacks[a]	Neighborhood Outlier Factor	[46]
	Class accuracy, Detection rate, False alarm rate	[14,15,20]
	ROC curve	[47]
	Class accuracy, detection rate, false-positive rate	[48,49]
UNS-NB15 Attacks[a]	Class accuracy, detection rate, false positive rate	[17,48]
ADFA attacks (Privilege escalation/system manipulation, data exfiltration)	ROC curve/Detection rate	[50–52]
ARP-based MITM,Modbus-query flooding; ICMP flooding; TCP-SYN flooding	Class Accuracy	[53]
DOS, Sensor injection attack	Reliability parameter	[42]
Man-in-the-middle (MITM)	Detection rate	[54]
Reconnaisance, Naïve and complex injection attacks	Kappa statistics; detection speed	[45,55]
	Classification accuracy; False positive rates; Confusion Matrix; Kappa statistics	[22,56]
Command injection, relay settings change, data injection.	Detection rate, False positive rate	[57,58]
Single and multiple-stage, multi-point attacks	ROC curve;	[59,60]

[a] The attack categories in this dataset are presented in Table 4.

subjective or based on convenience. Hence, a detailed analysis of the dataset for suitability is recommended, as diverse data collection methods were implemented for the datasets [88]. Hence, the computing domain, network protocol, simulated threat models, attack path, attack sequence, and originality are some of the considerations critical to the successful utilization of these resources for building a robust intrusion detection system.

4.1. IDS performance metrics and evaluation testbeds

Common ML algorithm performance evaluation technique computes the number of false alarms generated (percentage of false positive), classification accuracy, detection rate, or statistical performance measurements. To generally define the percentage of correctly classified instances among the total number of instances, commonly applied ML IDS evaluation methods are the detection rate (DT), true positive (TP), false positive(FP), true negative (TN), and false-negative (FN). Based on the constraints defined above for critical infrastructure, the selection of any of these metrics is highly subjective and situation driven. The Receiver Operating Characteristics curve (ROC), is one of the most widely used evaluation metrics. It is a plot of a false-positive rate versus the sensitivity, with the area under the curve reported as a good measure of an algorithm's classification performance. However, the ROC curve is a weak metric for IDS evaluation [78]. Table 5 shows some of the performance evaluation approaches for certain IDS techniques.

Although comparison of different IDS methods is difficult because the datasets for either network-based or process-based IDSs for major critical systems are not available, there are research efforts towards ML algorithm performance evaluation using a single platform such as Waikato environment for knowledge analysis (WEKA) [89] and testbeds for the development and validation of cybersecurity solutions [12]. Most testbeds consist of some switches, process monitors and PLCs to mimic small-scale industrial SCADA systems, with the capability to detect several network layer attacks such as DoS, port scanning, spoofing, etc. Research that evaluates common models built by respective evolutionary algorithms for data mining problems using knowledge extraction based on evolutionary learning (KEEL), WEKA and Rapid Miner (RM) ML data mining tools have been conducted [90]. Although limited in scope, a significant difference was reported for model output from each tool. Apart from data reliability issues, extending such research to cover critical infrastructure requires careful consideration of the nuances in the generated data.

5. Discussion and recommendation

Predicting and responding to assault against cyber-physical systems is an art because of the range of novelty involved in cyber-attacks. Moreover, the fuzziness of the attack surface, modernization, and sophistication of the attack or the threat actors also make the defense of the industrial control system a challenge. Most critical is the non-parametric characteristic of the cyber attacker and the physical consequence of a successful attack on ICS

with increasingly short detection and response time before the adversary violates the monitored system. Application of data-driven tools to the monitoring and detection of cyber-attack comes with a lot of promises. However, the rate of false alarm generated in real-world applications is a serious issue. In the development of a robust SCADA defense system, the questions about the influence of diverse cause of abnormal occurrence on the rate of false alarm generated by the IDS needs to be addressed. A critical analysis is needed to establish the nuances between different industrial control system configurations, the process behavior, component and its failure conditions, control principles, and how process knowledge could aid a successful attack.

Dataset lifespan is being shortened and "benchmark" datasets are fast becoming obsolete because threat actors are highly dynamic and sophisticated, and the corresponding upgrade in modern systems generate different data composition. Developing a new, comprehensive dataset requires detailed consideration for modern attack surface and well-defined dataset structure. Performing extensive evaluation of the system to obtain a robust dataset that considers zero-day and other modern exploits are expensive. Extending such consideration to different network architecture present further difficulties. In the absence of a robust historical database for specific real-world SCADA intrusions, establishing unified criteria to evaluate the effectiveness of existing IDS is difficult.

Also, proper development and implementation of a data-driven algorithm that seeks to identify and localize attacks based on dataset require a certain level of domain expertise. We observed some knowledge gaps in the development of ML algorithms. Multidisciplinary approach and domain knowledge are crucial to precisely define the expected operating conditions, analyze the available data, distill the output result, evaluate the performance of the algorithm, and characterize the nature of the detected anomalies. That is, the selection of appropriate dataset suitable for certain application require domain expertise. First, we observed that different data segmentation and selection methods are implemented to process data for algorithm development. Some researchers randomly select features or instances of data from the database for training the algorithm. Testing is done by another round of randomly selected features or instances, while others used the whole dataset for training and evaluating the algorithm. In the works of literature reviewed, no study describes the effect of these data sampling methods on the performance of the algorithm. For instance, an algorithm trained with large data size has been proven to present better performance than those trained on a small data set [46]. Despite prior evidence, worse algorithm performance with a larger dataset has been reported [22]. This lack of domain expertise and oversight in requisite preprocessing that goes into building an effective decision engine has limited the application of these engines in real systems. Secondly, most studies do not present a hyper-parameter selection method or optimization technique for the model, while some studies have no cognitive justification for the data preprocessing technique or model evaluation method used. Although we found some dated research that discusses issues on testing intrusion detection systems [91], we recommend a new study in this area, considering the rate of development in this field.

Moreover, efforts need to be directed to address the issues that constraints extensive evaluation of available algorithms. For instance, the performance of IDS built on data from privately owned protocol-specific testbeds cannot be independently repeated. Also, testing a model developed with data from a different SCADA configuration may not scale well on these testbeds. Besides, deploying such an intrusion detection model on production SCADA may result in high false negatives. This is because some interactions occur in a production SCADA that may not be well represented in testbeds. For instance, in a pressurized water nuclear power plant, the process control network is directly connected to critical programmable logic controllers and other subnetworks that handle information flow for the controllers that control the reactor, steam generator, feedwater flow, and the turbine. The scale of data exchange on such a process control network would be difficult to simulate using small scale testbeds. Also, the complex routine interaction that occurs between the connected components add an extra signature that needs to be considered to establish a robust testbed. Nevertheless, a good start is the development of open-source, high-fidelity, large-scale testbeds or SCADA virtual architectures, network and system simulators and programmable logic controllers to design, test and validate these algorithms [82,92,93]. A predictable issue with publicly available SCADA virtual architecture is that this architecture is also available to attackers to test their exploits, which present a cyber defense as a second-order chaotic problem. False-positive can be triggered intentionally by attackers with knowledge of the specially crafted data manipulation to feed into the system.

Consequently, it is necessary to develop a comprehensive abnormal occurrence detection system. We propose a dedicated private virtual machine or a "digital twin" with the capability to utilize real-time data from complex processes and reproducing a functional representation of the process, suitable for testing and evaluating the performances of a dedicated intrusion detection system without interrupting the real process. At the core of the digital twin is the development of a high-fidelity data-driven prototype of industrial machines and components. This virtual prototype is developed fully based on the physical pair, and runs in parallel with the physical system, enabling real-time condition monitoring, change detection, and process optimization. It can be developed as a virtual prototype of the nuclear power plant, enabling functional verification, virtual commissioning, and system performance analysis before, during, or after maintenance or major component changes. This allows for rapid task-planning and testing in the virtual world before any system changes are made to the physical plant.

There are two possible implementations of the digital twin:

1. Design (information/knowledge-driven): This approach involves developing a high-fidelity virtual prototype of the physical system using a database containing detailed design information, inspection information, maintenance, and service records, among others. This information is used to develop a simulation model that runs in-line with the physical system.
2. Data-driven: The data-driven approach involves utilizing real-time sensor values and parametric data as the input to the model. The model could be developed using deep learning or other machine learning algorithms. The parametric data with real-time process information are used to dynamically train the model, and the predictive output of the model is used as the prediction for the next sensor reading.

The capability of this digital twin could be extended to recognizing the nuances between random system faults, cyber events, and other anomaly initiators. Functionally, the system will explore the dependency effect of process change and network traffic data to effectively classify process change resulting from system fault and cyber-attack. This ultimately tends towards a re-designed resilient ICS with the capacity to perform an important safety function under cyber-attacks and incipient faults. This system will possess a mechanism to detect system faults and cyber-attacks independently while using redundant reconfiguration to achieve safety functions if the control system is under attack. Since process

variables deviate due to different reasons, weights could be attached to reduce the contribution of this consideration in the final intrusion detection output. Real-time implementation of this system is critical, to eliminate manual network traffic data sorting and additional pre-processes expertise.

6. Conclusion

A robust and sufficient security solution demands a comprehensive consideration of all critical interactions in the systems. Detecting process-level attacks targeting loss of SCADA process visibility or manipulating critical process parameters is not considered by many IDS proposals. This results in user-dependent monitoring systems with a high false alarm rate and low reliability. A framework to integrate process level constraints with network-level needs has been implemented. However, the works did not consider the complexity that characterizes industrial control systems, resulting in process changes for different operating states and initiating events.

In this work, we argue that the major contribution to the false alarm generation is the failure to identify and differentiate between the inherently similar signature that defines normal transients common to a complex system, incipient/slowly-developing fault and cyber intrusion with physical impact on the process information. To support our argument, we discuss nuclear plant control system characteristics that account for observed process measurement change and high false alarm rate for the intrusion detection system applied to detect intrusions on industrial controllers. Also, to aid IDS development and evaluation, we presented available synthetic and real industrial control systems data repositories. To significantly reduce the amount of nuisance alarm generated, we recommended an approach that considers the nuances in the data used in the development of machine learning algorithms. The present findings and recommended course of action serve as a foundation for the development of robust IDS with a significant reduction in the false alarm problem common to current intrusion detection systems.

Declaration of competing interest

We declare no conflict of interest for this submission.

Acknowledgements

This work was supported by the project of State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment (No.KA2019.418), the Foundation of Science and Technology on Reactor System Design Technology Laboratory (HT-KFKT-14-2017003), the technical support project for Suzhou Nuclear Power Research Institute (SNPI) (No. 029-GN-B-2018-C45-P.0.99–00003), and the project of the Research Institute of Nuclear Power Operation (No. RIN180149-SCCG.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.net.2020.05.012.

References

[1] J.P. Farwell, R. Rohozinski, Stuxnet and the future of cyber war, Survival 53 (2011) 23–40.
[2] B. Kesler, The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010, Strategic Insights, Spring, 2011, p. 2011.
[3] J. Stamp, et al., Common Vulnerabilities in Critical Infrastructure Control Systems. SAND2003-1772C, Sandia National Laboratories, 2003.
[4] O. Gonda, Understanding the Threat to SCADA Networks, Network Security, 2014, pp. 17–18, 2014.
[5] A. Rezai, et al., Key management issue in SCADA networks: a review. Engineering science and technology, Int. J. 20 (2017) 354–363.
[6] D.E. Mann, S.M. Christey, Towards a Common Enumeration of Vulnerabilities, 1999.
[7] P. Mell, T. Grance, ICAT Metabase CVE Vulnerability Search Engine, National Institute of Standards and Technology, 2002.
[8] P. Mell, T. Grance, Use of the Common Vulnerabilities and Exposures (Cve) Vulnerability Naming Scheme, NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV, 2002.
[9] S. Nazir, et al., Assessing and augmenting SCADA cyber security: a survey of techniques, Comput. Secur. 70 (2017) 436–454.
[10] A. Carcano, et al., Scada malware, a proof of concept, in: International Workshop on Critical Information Infrastructures Security, 2008.
[11] A.A. Akinola, et al., Cyber-security evaluation for a hypothetical nuclear power plant using the attack tree method, J. Phys. Secur. 8 (2015) 19–36.
[12] T. Cruz, et al., A cybersecurity detection framework for supervisory control and data acquisition systems, IEEE Trans. Indust. Inf. 12 (2016) 2236–2246.
[13] A. Scott, Tactical Data Diodes in Industrial Automation and Control Systems, SANS Institute InfoSec Reading Room, 2015, pp. 1–32.
[14] M.R. Gauthama Raman, et al., An efficient intrusion detection system based on hypergraph - genetic algorithm for parameter optimization and feature selection in support vector machine, Knowl. Base Syst. 134 (2017) 1–12.
[15] S. Mukkamala, et al., Intrusion detection using an ensemble of intelligent paradigms, J. Netw. Comput. Appl. 28 (2005) 167–182.
[16] L.A. Maglaras, J. Jiang, A novel intrusion detection method based on OCSVM and K-means recursive clustering, ICST Trans. Secur. Saf. 2 (2015) e5.
[17] A. Almalawi, et al., An Unsupervised Anomaly-Based Detection Approach for Integrity Attacks on SCADA Systems. Computers & Security, vol. 46, 2014, pp. 94–110.
[18] J. Hu, et al., A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection, IEEE network 23 (2009) 42–47.
[19] W. Hu, et al., Online adaboost-based parameterized methods for dynamic distributed network intrusion detection, IEEE Trans. Cybern. 44 (2013) 66–82.
[20] R.A.R. Ashfaq, et al., Fuzziness based semi-supervised learning approach for intrusion detection system, Inf. Sci. 378 (2017) 484–497.
[21] S. Elhag, et al., On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems, Expert Syst. Appl. 42 (2015) 193–202.
[22] L. Zhou, et al., Automatic fine-grained access control in SCADA by machine learning, Future Generat. Comput. Syst. 93 (2019) 548–559.
[23] T. Alves, et al., Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers, IEEE Embedded Syst. Lett. 10 (2018) 99–102.
[24] P. Nader, et al., ${l_p} $-norms in one-class classification for intrusion detection in SCADA systems, IEEE Trans. Indust. Inf. 10 (2014) 2308–2317.
[25] H. Hota, A.K. Shrivas, Data mining approach for developing various models based on types of attack and feature selection as intrusion detection systems (IDS), in: Intelligent Computing, Networking, and Informatics, Springer, New Delhi, 2014, pp. 845–851.
[26] G. Kumar, K. Kumar, Design of an evolutionary approach for intrusion detection, Sci. World J. 2013 (2013), https://doi.org/10.1155/2013/962185.
[27] A.A. Aburomman, M.B.I. Reaz, A survey of intrusion detection systems based on ensemble and hybrid classifiers, Comput. Secur. 65 (2017) 135–152.
[28] A. Ayodeji, et al., Knowledge base operator support system for nuclear power plant fault diagnosis, Prog. Nucl. Energy 105 (2018) 42–50.
[29] W.-C. Lin, et al., CANN: an intrusion detection system based on combining cluster centers and nearest neighbors, Knowl. Base Syst. 78 (2015) 13–21.
[30] A. Ayodeji, Y.-k. Liu, Support vector ensemble for incipient fault diagnosis in nuclear plant components, Nucl. Eng. Technol. 50 (2018) 1306–1313.
[31] A. Ayodeji, Y.-k. Liu, SVR optimization with soft computing algorithms for incipient SGTR diagnosis, Ann. Nucl. Energy 121 (2018) 89–100.
[32] A.L. Buczak, E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Commun. Surv. Tutorials 18 (2015) 1153–1176.
[33] S.X. Wu, W. Banzhaf, The use of computational intelligence in intrusion detection systems: a review, Appl. Soft Comput. 10 (2010) 1–35.
[34] J. Nivethan, M. Papa, A SCADA intrusion detection framework that incorporates process semantics, in: Proceedings of the 11th Annual Cyber and Information Security Research Conference, 2016.
[35] O. Linda, et al., Neural network based intrusion detection system for critical infrastructures, in: 2009 International Joint Conference on Neural Networks, 2009.
[36] O. Linda, et al., Towards resilient critical infrastructures: application of type-2 fuzzy logic in embedded network security cyber sensor, in: 2011 4th International Symposium on Resilient Control Systems, 2011.
[37] T.T. Nguyen, G.J. Armitage, A survey of techniques for internet traffic classification using machine learning, IEEE Commun. Surv. Tutorials 10 (2008) 56–76.
[38] W. Li, et al., False sequential logic attack on SCADA system and its physical impact analysis, Comput. Secur. 58 (2016) 149–159.
[39] A. Robles-Durazno, et al., A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system, in: 2018 International Conference on Cyber Security and Protection of Digital

Services. Glasgow, UK,June 11-12, 2018.
[40] D. Hadžiosmanović, et al., Through the eye of the PLC: semantic security monitoring for industrial processes, in: Proceedings of the 30th Annual Computer Security Applications Conference. New Orleans, USA,December 8-12, 2014.
[41] I.N. Fovino, et al., Modbus/DNP3 state-based intrusion detection system, in: 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.
[42] X. Jie, et al., Anomaly behavior detection and reliability assessment of control systems based on association rules, Int. J. Critical Infrastruct. Protect. 22 (2018) 90–99.
[43] M. Krotofil, et al., The process matters: ensuring data veracity in cyber-physical systems, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. Singapore,April 14-17, 2015.
[44] F. Zhang, et al., Multi-layer data-driven cyber-attack detection system for industrial control systems based on network, system and process data, IEEE Trans. Indust. Inf. 15 (2019) 4362–4369, https://doi.org/10.1109/TII.2019.2891261.
[45] T. Morris, W. Gao, Industrial control system traffic data sets for intrusion detection research, in: International Conference on Critical Infrastructure Protection, 2014.
[46] J. Jabez, B. Muthukumar, Intrusion detection system (IDS): anomaly detection using outlier detection approach, Procedia Comput. Sci. 48 (2015) 338–346.
[47] G. Kim, et al., A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Syst. Appl. 41 (2014) 1690–1700.
[48] A.-H. Muna, et al., Identification of malicious activities in industrial internet of things based on deep learning models, J. Inf. Secur. Appl. 41 (2018) 1–11.
[49] S. Potluri, C. Diedrich, Deep feature extraction for multi-class intrusion detection in industrial control systems, Int. J. Comput. Theory Eng. 9 (2017) 374–379.
[50] G. Creech, Developing a High-Accuracy Cross Platform Host-Based Intrusion Detection System Capable of Reliably Detecting Zero-Day Attacks, University of New South Wales, Canberra, Australia, 2014.
[51] G. Creech, J. Hu, Generation of a new IDS test dataset: time to retire the KDD collection, in: 2013 IEEE Wireless Communications and Networking Conference (WCNC), 2013.
[52] B. Borisaniya, D. Patel, Evaluation of modified vector space representation using adfa-ld and adfa-wd datasets, J. Inf. Secur. 6 (2015) 250.
[53] I. Frazão, et al., Denial of service attacks: detecting the frailties of machine learning algorithms in the classification process, in: International Conference on Critical Information Infrastructures Security. Kaunas, Lithuania,September 24-26, 2018.
[54] P. Nader, et al., Detection of cyberattacks in a water distribution system using machine learning techniques, in: 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC), 2016.
[55] J. Yeckle, S. Abdelwahed, An evaluation of selection method in the classification of scada datasets based on the characteristics of the data and priority of performance, in: Proceedings of the International Conference on Compute and Data Analysis. Florida, USA,May 19-23, 2017.
[56] I.P. Turnipseed, A New Scada Dataset for Intrusion Detection Research, Mississippi State University, 2015.
[57] M. Keshk, et al., Privacy preservation intrusion detection technique for SCADA systems, in: 2017 Military Communications and Information Systems Conference (MilCIS), IEEE, 2017.
[58] R.C.B. Hink, et al., Machine learning for power system disturbance and cyber-attack discrimination, in: 2014 7th International Symposium on Resilient Control Systems (ISRCS), 2014.
[59] M. Kravchik, A. Shabtai, Detecting cyber attacks in industrial control systems using convolutional neural networks, in: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. Toronto, ON, Canada,October 19, 2018.
[60] J. Goh, et al., Anomaly detection in cyber physical systems using recurrent neural networks, in: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE). Singapore,January 12-14, 2017.
[61] N. Erez, A. Wool, Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems, Int. J. Critical Infrastruct. Protect. 10 (2015) 59–70.
[62] D.I. Urbina, et al., in: Attacking Fieldbus Communications in ICS: Applications to the SWaT Testbed, SG-CRC, 2016.
[63] M. Ring et al., A Survey of Network-Based Intrusion Detection Data Sets. Arxiv Version (2019) arXiv:1903.02460vol. 2.
[64] A. Shiravi, et al., Toward developing a systematic approach to generate benchmark datasets for intrusion detection, Comput. Secur. 31 (2012) 357–374.
[65] Caida, Center for applied internet data analysis, Available from: http://www.caida.org/data2019 [cited 2019 07/08]. [Dataset].
[66] Unibs, Anonymized traces collected by U. Brescia Ground Truth (GT) software suite, Available from: http://netweb.ing.unibs.it/~ntw/tools/traces/2011 July 13, 2011 [cited 2019 07/08]. [Dataset].
[67] UMass, UMass trace repository, Available from: http://traces.cs.umass.edu/index.php/Main/HomePage2018 [cited 2019 07/08]. [Dataset].
[68] Nfnsm, Network forensic and network security monitoring PCAP repository, Available from: https://www.netresec.com/?page=PcapFiles2019 [cited 2019 07/08]. [Dataset].
[69] A.H.L. Iman Sharafaldin, Ali A. Ghorbani, A realistic cyber defense dataset: canadian institute for cybersecurity network traffic and log files, Available from: https://registry.opendata.aws/cse-cic-ids2018/2018 [Dataset].
[70] G. Grinstein, Internet exploration shootout (IES), Dataset Available from: http://ivpr.cs.uml.edu/shootout/network.html2001 [cited 2019 07/08]. [Dataset].
[71] U.o.N, Mexico, sequence-based Intrusion detection [cited 2019 07/08]; Available from: https://www.cs.unm.edu/~immsec/systemcalls.htm, 2019.
[72] I. Sharafaldin, et al., Toward generating a new intrusion detection dataset and intrusion traffic characterization, ICISSP (2018).
[73] D.a.G. Dua, C, UCI Machine Learning Repository. http://archive.ics.uci.edu/ml, 2019 [cited 2019 20/06].
[74] S. Hettich, S. Bay, The UCI KDD Archive, vol. 152, University of California. Department of Information and Computer Science, Irvine, CA, 1999. https://www.digitalbond.com/2019.
[75] M. Tavallaee, et al., A detailed analysis of the KDD CUP 99 data set, in: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.
[76] N. Moustafa, J. Slay, UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), in: 2015 Military Communications and Information Systems Conference (MilCIS), 2015.
[77] N. Moustafa, J. Slay, The evaluation of Network Anomaly Detection Systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set, Inf. Secur. J. A Glob. Perspect. 25 (2016) 18–31.
[78] J. McHugh, Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory, ACM Trans. Inf. Syst. Secur. 3 (2000) 262–294.
[79] P.S. Adhikari U, T. Morris, R. Borges, J. Beaver, ORNL industrial control system (ICS) cyber attack datasets, Available from: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets2018 [cited 2019 07-09].
[80] A.S. Laboratory, CTF-WP industrial control traffic, Available from: http://www.icsmaster.org/archives/ics/7412018 [cited 2019 07/09].
[81] S. Adepu, iTrust-SWaT Dataset, Available from: https://itrust.sutd.edu.sg/itrust-labs_datasets/ [cited 2019 07-11].
[82] T.I.C.s, Conference, 4SICS repositories, Available from: https://www.netresec.com/?page=PCAP4SICS2019 [cited 2019 07/08].
[83] D. Peterson, PCAP Files from the SCADA security scientific symposium 2015 (S4x15). Available from:: https://www.digitalbond.com/2019 [cited 2019 07/08].
[84] A. Lemay, J.M. Fernandez, Providing {SCADA} network data sets for intrusion detection research, in: 9th Workshop on Cyber Security Experimentation and Test ({CSET} 16), 2016 dataset available from: https://github.com/antoine-lemay/Modbus_dataset.
[85] J. Smith, A collection of ICS/SCADA PCAPs, Available from: https://github.com/automayt/ICS-pcap2019 [cited 2019 07/08].
[86] Darpa, DARPA intrusion detection evaluation on LLDOS and Windows NT, Available from: http://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets2000.
[87] L.B.N.L.a. Icsi, LBNL/ICSI enterprise tracing project, Available from: https://www.icir.org/enterprise-tracing/download.html2005.
[88] D. Zhou, et al., A survey on network data collection, J. Netw. Comput. Appl. 116 (2018) 9–23.
[89] M. Hall, et al., The WEKA data mining software: an update, ACM SIGKDD explorations newsletter 11 (2009) 10–18.
[90] M. Graczyk, et al., Comparative analysis of premises valuation models using KEEL, RapidMiner, and WEKA, in: International Conference on Computational Collective Intelligence, 2009.
[91] P. Mell, et al., An Overview of Issues in Testing Intrusion Detection Systems, 2003.
[92] T. Alves, T. Morris, OpenPLC: an IEC 61,131–3 compliant open source industrial controller for cyber security research, Comput. Secur. 78 (2018) 364–379.
[93] H. Holm, et al., A survey of industrial control system testbeds, in: Nordic Conference on Secure IT Systems, 2015.