Securing Industrial Control System Environments: The Missing Piece

Uchenna D Ani[1], **Nneka Daniel**[2], **Francisca Oladipo**[3,] **Sunday E Adewumi**[4]

u.p.ani@cranfield.ac.uk, agbanusin@gmail.com, francisca.oladipo@fulokoja.edu.ng, sunday.adewumi@fulokoja.edu.ng

[1] *Manufacturing Informatics Centre, Cranfield University, United Kingdom.*
[2]*H. Pierson Associates Ltd, Lagos-Nigeria*
[3,4] *Department of Computer Science, Federal University Lokoja.*

Abstract

Cyber-attacks on Industrial Control Systems (ICS) are no longer matters of anticipation. Industrial infrastructures are continually being targeted by malicious cyber actors with very little resistance on their paths. From network breaches to data theft, denial of service attacks to privilege escalation; command and control functions have in some way been exerted on targeted industrial systems. Safety, security, resilience, reliability and performance require private industrial control system user organizations and the public sector to device strategies and steps towards dealing decisively to these emerging and increasing ICS cyber security concerns. There are already couple security solutions proposed by governments, private organizations, academia, and industries for achieving this goal. This discourse reviews the ICS security risk landscape, current security strategies and solutions with a view to discovering the gaps or weaknesses in the effective mitigation of cyber-attacks, and the enhancement of cyber security. Notable fissures in existing ICS security solutions include: greater emphasis on technology security while discounting other critical bits like people and processes, which is clearly incongruent with emerging security threats and attack trends, the unilateral dimension strategy towards security which focuses more on SCADA systems, and the emergence of more sector-specific solutions as against generic security solutions. Better solutions include approaches that follow similar evolutionary patterns as the problem trend. These include cyber security measures that would embrace constant evolution in response to changes in the threat, vulnerabilities, attacks, and impact domains. Solutions that recognise and capture; people, process, and technology security enhancement into a single system entity with holistic provisioning that can meet all three-entity vulnerabilities for a more secured ICS environment.

Keywords:
Cyber Security, SCADA Security, Cyber-physical Security, ICS Security, Security Standards,

1. Introduction

In time past, security for Industrial Control Systems (ICSs) was hardly an issue because of the relative isolation and presumable seclusion of such networks from external interference. Legacy devices and protocols were in use, which worked only among families if the same architecture, hence did not require any interfacing with open technologies. As technology trends unfold, the quest to sustain relevance while improving industrial capabilities in productivity and service delivery also grew and paved way for the incorporation of information technology (IT) and telecommunications infrastructureS into mainstream ICS [1], [2]. Open standards-enabled computing hardware, software, operating systems, and network protocols are replacing the prior, fashionable, branded ICS components, and has transformed the typical operational technology (OT) systems into nearly conventional IT systems. Although quite rewarding as desired, the IT-OT convergence exposes ICSs to a great deal of both internal and external cyber security risks (threats, vulnerabilities, attacks, and impacts) [2]–[4].

The aftermath is that today; cyber-attacks and incidents on ICSs have becomes realities. ICS infrastructures are continually being targeted by malicious cyber actors with very little resistance and force to oppose them. ICS network breaches, theft operational data, denial of service attacks, privilege escalation, and command and control functions are among the plethora of recorded compromises which been exerted on targeted ICSs. Ensuring IC environment security, resilience, safety, reliability, and

performance require both public and private sector organizations and stakeholders within the ICS community to device strategies and steps towards addressing the emerging cyber security concerns. This has not been left unattended, as there are already available research works and solutions put forwards by governments, private organizations, academia, and industries for addressing the security challenge. However, the confidence desired for developing and adopting these emerging security solution approaches does not appear to have increased, but rather continued to dwindle, evidenced by the continued upsurge in cyber incidents targeting ICS networks and environments. We think that for this scenario to persist despite existing solution effort out there, something is certainly not right around the challenges and the solutions available which leads to the thoughtful question: '*what may be missing in the current ICS security solution landscape?*'

In this paper, we attempt to answer the above question by examining existing and available security strategies and solutions for controlling and mitigating cyber-attacks and incidences and enhancing security on ICSs. This goal will be achieved by: (i) identifying common security principles and requirements relevant and applicable for ICS security, (ii) highlighting the trends in ICS cyber attacks and incidents, (iii) highlighting the common viewpoints related to ICS security threats, vulnerabilities, and impacts, (iv) providing a reference resource on the common and available security implementation techniques and approaches to ICS security researchers, developers, and system owners, and (v) identifying the limitations in existing ICS security approaches and providing information and directions for possible future research that can yield better ICS security solutions. This work will be beneficial to security analysts, developers, and auditors responsible for securing industrial control systems by providing them information relating to the varied techniques security is being conceived and implemented and possibly techniques for improvement. It will also be beneficial to industrial control system security risk administrators, managers, and top executives by informing them of growing trends in security applications, decision-making relative to the choice of appropriate security approach that can suite their unique security requirements. In this paper; 'security' and 'cyber security' are used interchangeably, and used to mean the same.

In Figure 1, the inter-sectional relationship amongst the contexts reviewed is presented. This also defines flow of information presentation as contained in this paper. By this flow of information, this resource aims to provide a structured view and understanding of the deficiency(ies) in existing security approaches for ICS, and to support well-informed decision-making related to the selection and adoption of appropriate security solutions or their enhancements.

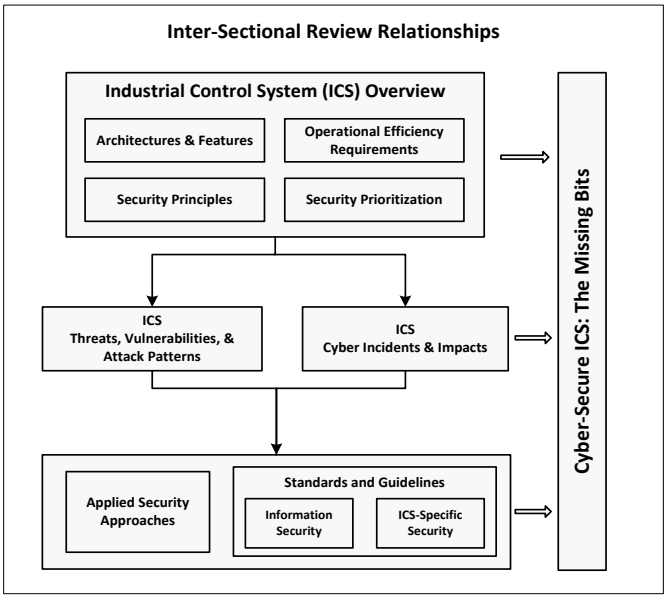

Figure 1: Relationship among reviewed sections

The remaining part of this paper are structured as follows: Section 2 presents an overview of ICS and relative principles and requirements for security as viewed in prior literatures, and the enablers of security issues in the industrial control system environment. Section 3 discusses ICS security risks in relations to threats, vulnerabilities, actual attacks incidents and associated patterns, and the nature of impacts. Section 4 reviews the common technical security approaches adopted in research for protecting ICS from cyber-attacks and intrusion, and analysis of the limitations. Section 5 discusses the possible issues that can be drawn from the current security approaches commonly adopted, and their implications to overall system security. Section 6 presents a conclusion and recommendation related to future security solutions areas that can enhance security for ICSs.

2. Industrial Control Systems Environments

ICS are a system of operational elements typically found in critical infrastructures environments (e.g. manufacturing, transport, electrical, energy, oil and gas, chemical, pharmaceutical, food and beverages, water and wastewater) used to control and monitor industrial processes to achieve industrial and business objectives [5], [6]. The operational elements of ICS typically include technologies such as control devices, actuators, sensors, human-machine-interfaces, remote diagnostic devices, storage data historians, corporate network and internet connections [7]. Other elements typically found in ICS environments include; people (human agents) and processes [8].

Essentially, control, monitoring, distribution, and management form the basic functions of an ICS. These functions are undertaken in part or whole by elements or constituents within the ICS environment. A typical ICS consist of people using technologies to control, monitor, and(or) manipulate industrial processes. Processes help to bring about the desired industrial objective such as production or distribution. Technologies (devices) help to implement and drive the actualization of defined processes. People are there to control, monitor, attest, and respond appropriately to operational reliability behaviours, functionality of technologies, and the underlying process they implement. A key characteristic of ICSs is that the constituent elements i.e., people, process, and technologies (especially related to components and functionalities) are often highly interconnected and mutually dependent on each other for normal and effective operations with high criticality, so that any form of disruption on one component can have a rapid, huge, and devastating effects on other dependent components, and potentially the society.

2.1 ICS Security Principles and Requirements

The basics of ICS security is drawn from traditional Information Technology (IT) systems, although the critical nature of ICS processes emphasizes even stricter service and security requirements when compared to IT systems. For example, from a Quality of Service perspective, *'Determinism'* describes a requirement for network signal speed and reliability with low or nearly zero latency or jitter [9]. This is not so much the in the case of IT networks as some degree of latency can be tolerated and may not significantly and noticeably affect the operations of the system. Security assurance in the IT is generally emphasized in terms of three primary principles in that order; *Confidentiality* (C), *Integrity* (I), and *Availability* (A) [10]–[14].

Availability underscores that the flow and delivery of systems services and data are not impaired or interrupted, and are reachable when required [10]. For ICS, it means the continuous access and use of information services, and ensuring that all system components must functioning successively and appropriately [15], [16]. For this reason, availability is considered the most priority requirement in ICS. ICS systems are essentially high-availability systems. *Integrity* in ICS highlights that a design or process system performs in the mode it is intended without alterations [10]. In ICS, integrity is violated when an unauthorised modification is made on any data, process, procedures, or outcomes, such that another results which is non representative of the desired emerges. In the ranking of priority, integrity is next after availability. *Confidentiality* enforces only authorised restrictions on information access, shielding against disclosures to unlawful individual or systems [10], [17]. In ICS, it demands the preservation of industrial asset; designs, processes, quality controls, supply chain, personnel, data, and devices, from access by unauthorised or external entities. This is very critical to modern industrialization, as a

disclosure of business and (or) industry-critical asset or intellectual property to competitors and adversaries could yield a loss of competitive advantage, and ultimately industrial or market reputation.

Nevertheless, it is commonly viewed and acknowledged that attaining absolute security even for IT system is difficult and potentially infeasbility at least at the moment. This is for a couple of reasons. Firstly, the limitation of developer fallibility and exploitation, which brings in the recurrent likelihood of making mistakes and such being abused by threat actors. Secondly, the total implementation and enforcement of either of these security principles could in themselves lead to security violations of the others. For instance, the application of extreme restrictions in ICS to uphold confidentiality or integrity could cause a loss of availability, which is of topmost priority. On the other hand, ensuring absolute availaibility will mean that confidentiality and integrity enforcements may require some compromise. Typically, the solutions often end up as trade-off for the most desired security property that protects the most critical part of asset of the system, or that helps achieve the most desired security objective of the system. In the end, it ends as balance between security and functionality.

However, the AIC (availability, integrity, and confidentiality) security triads have been noted to be too focused on securing technology elements, and not enough to protect other elements such as people and process [18], also IAC implementation are often more polarised towards the preventive approach that is presumably non-holistic and unsuitable for ICS environment. Consequently, other researches have suggested additional security principles in a bid to address the limitations of AIC and to keep up with the dynamics in the way security is viewed and addressed. In response to the lag emphasis on human-level security considerations, three additional security principles: authenticity, possession, and utility to be added to the AIC triads, which can also be quite useful if considered in the ICS context. Together, these are reffered to as the Parkerian Hexad process [18].

Authenticity emphasises the guarantee that a message, transaction, or other exchange of information is actually from the source it claims to be from. Essentially, it involves proof of identity [18]. In the context, it involves the substantiation of all ICS-related processes like sensing, communications and actuation, and their respective initiators, emphasizing unpretentious data, transactions and communications within any computing system or process [15], [19]. *Possession* emphasises guarding against the notion and possibility of possessing and controlling confidential data by an unauthorized party without actually violating confidentiality. Hence, Possession is crucial because it covers security violations where confidentiality is both significant and non-existent [18]. In ICS, it would mean that a protective capability be enabled such that would make it difficult or impossible to view and access process data contents even if the means is accessible. *Utility* refers to the usefulness of data, which in the context of ICS would mean that process data should always be in their useful state [18].

More contextually, research articles discoursing security considerations relating to ICS, cyber-physical systems, and Industrial Internet-of-Things (IIoT) also differ in their proposition and adoption of relevant security principles. *Accountability* and *Non-repudiation* have been proposed [13] as secondary security principles that should be considered towards improving cyber security in ICS, and even in traditional IT environments; on the argurement that users must be able to assume responsibility for their actions. There are further arguments supporting the consolidation of security sufficiency in principles for ICS [20] [10] [15]. *Authenticity* as a security principle is recommended for inclusion into ICS security requirements [15]. Authors concur that authenticity is a significant security requirement for any computing and communication process [19], arguing that its relevance in ICS ensures the substantiation of all ICS-related processes like sensing, communications and actuation, and their respective initiators. It emphasizes unassuming data, transactions and communications within any computing system or process.

Veracity is also presented in [21]; reflecting the ability of a system or entity to evade a deception attacks; in relation to integrity. In ICS, this translates to ensuring process and control instructions are correctly captured from control algorithm executions without fear of misguidance from external sources. *Timeliness* and *Graceful Degradation* have also been proposed emanating from basic ICS features [22]. Timeliness emphasizes that any demanded, reported, and distributed information should not be obsolete

but correspond to real-time. The system should be able and subtle enough to process requests of normal and (or) legitimate human intervention in an appropriate fashion. *Graceful Degradation* on the other hand, loads on the system the ability to localize attack impacts, suppressing contaminated data flow within contaminated region to avoid further escalation onto a wider scope. *Reliability* is discussed to emphasise an ability to perform intended function(s) for a given period of time under a given set of conditions [23], [24], [25], [26]. *Robustness* property is also prescribed in literatures as relevant. It emphasises the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environment conditions [27], [28], [29]. *Trustworthiness* is also proposed by researchers as a relevant security principle. It is described as the extent to which a system can be relied upon to perform exclusively and correctly the system task(s) under defined operational and environmental conditions over a defined period of time, or at a given instant in time [30], [31], [32], [33], [34], [35].

Above all, Safety is also a critically requirement in ICSs [36]. This requirement can also be easily deduced from the definition of 'security' from NIST SP 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security [37]. Here, security is defined as: "freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment". Typically, Safety takes precedence over security in ICS environments. Any security measure(s) that weaken(s) safety is unacceptable [37]. Cyber security guards ICSs, and keeps industrial processes and operations running safely and efficiently. It ensures that data and process instructions remain uncompromised, communication flows and exchanges uninterrupted, and malicious codes and applications barred from infecting control systems and networks, or upsetting control and processes.

As it appears, security principles, properties or requirements are indeed numerous and diverse. The contexts of functions and operational objectives would typically determine what an associated security requirement would be. It is also not feasible to implement and enforce all of the mentioned principles within a single system as earlier discussed. A form of priority ordering would be the best way to go as in the case of AIC in ICS [38], [39] in [10]. The choice of principles should always go in line with clear component, process, or system criticality indicators, and target objectives, thus, ensuring that priority emphasis veer towards the most operations/business relevant security principles. A good example is the swing towards availability for manufacturing, which indicates that there is greater value attachment to information on ICS, processing overhead, protocol supportability [10], and information assurance [17]. And while IT systems and ICS share resemblances, nonetheless, differences in designs and operational goals make one system different from the other. It thus make sense to construe that both systems would not have the same principle emphasis in terms of cyber security. Security administrators, managers, and analysts are required to first understand the basic setup and operations of their ICS, characterise risks in relations to technologies, people, and process elements to help determine which security principles may be relevant and required for implementation, including and understanding of the extent to which implementation need to be carried out out to maintain operations. The security principles discussed are however, worth considering especially with the gradual adoption of IoT into ICS networks and other critical national infrastructures that are ICS-driven.

2.2 Enablers of Security Issues in Industrial Control System Domain

ICS were initially developed essentially with operational objective in mind, much of which linked to performance and productivity. Security or cyber security was far from being a design requirement. Individual companies and vendors developed custom proprietary standards and protocols to ensure the attainment of their operational objectives, and there were over 150 of such functional protocols that upheld performance and productivity, but lacked security capabilities. Thus, their use in ICS networks and systems contribute to the emergence of security vulnerabilities and issues. Some of the most popular protocols include: MODBUS/TCP, DNP3, and PROFIBUS. Summary features of these protocols and few others are presented in Table 1.

Table 1: Common Industrial Control Systems Protocols

Protocols	Organisation/Standard	Main features
MODBUS TCP/IP	MODBUS-IDA (www.modbus.org)	Encapsulates fieldbus packets over TCP; attempting to become an IETF standard
DNP3	(IEC) Technical Committee 57, Working Group 03 standard	It is also a based on the 3-layer OSI model
PROFIBUS	Type 3 protocol of IEC Standard 11674 and 61158 (www.profibus.org)	3-layer OSI model; has extensions for safety features; ProfiNet version provides Ethernet compatibility
Ethernet/IP (Industrial Protocol)	Open DeviceNet Vendors Association (ODVA) (www.odva.org)	Object-oriented, protocol; provides interoperability over Ethernet and fieldbus networks
DeviceNet	Open DeviceNet Vendors Association (ODVA) (www.odva.org	Belongs to the CIP (Control and Information Protocol) family; CAN protocol defines layers 1 & 2; the rest are defined by DeviceNet and CIP
ControlNet	ControlNet International (www.controlnet.org)	Belongs to the same CIP (Control and Information Protocol) family; new physical layer with higher speed, strict determinism and repeatability with greater range
Foundation Fieldbus	The Fieldbus Foundation/open standard protocol (www.fieldbus.org)	Incorporates many safety features that make it a good candidate for mission-critical applications

Other vulnerability enablers are quite procedural and relate to how these ICS protocols listed in Table 1 are developed and released for wider use. As can be observed, the ke features of the protocols listed seem to favour functional and operational performances such as improvement of processing speed, determinism, and repeatability and safety among others. Emphasis are more focused on achieving compatibility with IT/Ethernet procols and interoperability with IT systems. These, ICS protocols mostly do no undergo extensive security testing for robustness, thus do not directly account for any security features or capabilities as would be seen. These proprietary communication protocols are thus considered inherently insecure. For instance; Modbus was formerly developed for serial line communication, today; Modbus/TCP implementations are commonly used in ICSs. Modbus and DNP3 protocols currently do not support authentication, integrity checking, authorization or encryption. As a result, design flaws in the core protocols render ICS insecure [40], [41]. Hence, the use of the most basic scanning penetration test tools usually yield several exploitable vulnerabilities. Research records [42]–[44] show the potentials for crashing ICS components just be simply establishing connection with TCP ports on an ICS device. Additionally, ping sweeps have caused devices to behave away from expectations [45]. Thus, if ICS infrastructures have to be tested, the test must be done cautiously to avoid system damage or disruption.

Most ICS devices supporting the vulnerable protocols are now supporting web-enabled capabilities, even without stronger authentication beyond passwords. Even passwords on default are usually very weak and could be easily broken. Thus, current ICS authentication methods are not seen to be commensurate to the criticality level of the system. In most cases, there are very minimal access controls between the corporate network and the control system [46], and an attacker only needs to compromise the corporate network to get to the control system network.

It is vital to recognise that with the current complex inter-networked technology of ICS, there abound multiple access points to any of such network where system devices have weak or virtually no security capacities. The notion of being inaccessible to cyber attackers on the bases of ‘security-by-isolation’ has become illusionary and must be disabused from the minds of today ICS operators. ICS users and operators need to be further enlightened on the reality that increased integration with IT infrastructure and connectivity corporate networks have altered the formerly isolated network architecture of ICS, and formed a larger, wider, and complex inter-networked environment. As it is now, physical ‘air-gapping’ does not guarantee network security. So long as there are the likes of gateways, some form of connection to the outside world (dial ups, or internet), commercially-off-the-shelf devices, open

standards, and or protocols, determined attacks will always find exploit mediums to get to any machine on the ICS [47].

3. Security Risks in ICS

3.1 Security Threats and Vulnerabilities

It has been affirmed in [3], and indeed well proven by the cyber security antecedents that faults and flops in ICSs can greatly pose substantial risks to; health and safety of humans, severe impairment to the environment, and economic impacts such as production losses, harm to the industry and by extension the nation's economy, and illegal disclosure of proprietary information. Threat agents could include both insiders and outsiders bearing disgruntles, greedy or malicious intents. Extremist, terrorists, and nation-state actors are also potential threats when considered in the context of critical national infrastructures [48], and industrial organisations must be aware of these varied threat groups and the potential intents or motivations that might drive their actions. Some of which include, espionage, process manipulation, system hijack or shutdown, system sabotage or information stealing [8].

Broadly speaking, ICS cyber threats factors could be considered in relation to the elements that constitute the system. These include: people, process and technology [8]. It means that cyber threats tend to target one or more of these elements to achieved a successful sabotage. It is reasonable to assume that vulnerability and risk factors relative to the three elements (people, process, and technology) should all contribute to the massive pool of threat forms that can be considered in ICS. People-related vulnerabilities emerge as lack sufficient security knowledge and skills, which can in turn influence fear, misjudgements, misperception, errors in actions and inactions. Process-related vulnerabilities can be expressed in the form of; non approval or compliance to security policies, insufficient security policies, poor segregation of duties, lack of authentication and authorization policies, least user privilege violation, poor patch and change management, limited checking of security logs, Physical access (insufficiently controlled areas), insufficient incident response planning, and insufficient practicing of emergency situations. Technology-related vulnerabilities include: configuration and implementation errors, unpatched systems, lack of input validation and Weak user authentication,, buffer overflows and uninitialized memory, weak or badly implemented crypto (i.e., md2, md5, sha-1, now considered weak), external connections (e.g., extranets, internet, and dial-in/out modems connections), mobile and remote operators and vendors (remote access), deficiencies in remote support and access implementations (VPN), forgotten back-end modems, and growing usages of wireless (IEEE 802.11) and Bluetooth (field) devices, rogue devices and (unauthorized) laptops, limited use and usefulness of firewalls, intrusion detection systems (IDS), VPN or DMZ-network segments, firewall filtering deficiencies, and insufficient (application-level) firewall support for ICS communication protocols, usage of general enterprise systems (such as DNS and authentication services), and numerous attack points (widely, geographically dispersed infrastructure) [1]

However, amongst the three elements discussed; people (human element) are often noted to be the weakest spot in terms of security for certain reasons. Humans are inclined to retain limited imagination when it comes to security. Again, with specifics to ICS users; asset owners and operators are usually experts in engineering and automations rather than cyber security [1]. These incapacities are being exploited quite easily by intelligent adversaries to sabotage ICSs. The mixture of both legacy and open technologies in ICS has pave way for the proliferation of technology threats, while the non-adherence to defined processes and procedures concretises the emergence of process-oriented threats.

3.2 ICS Security Attacks, Patterns and Impacts

The usual focus on trustworthiness and performance of ICSe often account for the system's exclusivity in both hardware and software. So that it often infeasible to incorporate more highely secure components because of the potential operational constraints and impacts they may cause to the overall system. Taking the example of manufacturing control systems, potential threats or attacks can come

varied forms. Attacks can include jammed or delayed flow of service information through the manufacturing control networks to disrupt production-critical operations, illegal changes to service instructions, production commands, or alarm thresholds, capable of damaging, disabling, or worse; shutting down production lines or equipment, generating inimical environmental effects, or jeopardize human life. Wrong information can also be sent to system operators, either in disguise of unauthorized changes, or to influence inappropriate reactions from operators to cause destructive impacts. Modification of manufacturing control system software or configuration settings, or infection with malware; to cause damage to product/production quality [3]. Kaspersky's Lab's report on threat Landscapes for Industrial Automation Systems in H1 2017 indicated that the most widely adopted channel for cyber-attack perpetration on ICSs is the internet – perhaps enabled by unaware, unskilled or unsuspecting ICS operator attempts to download malware or access malicious phishing web resources [49]. The most probable reason why these have become feasible is due to the presenece of interfaces enbling communication between; (i) industrial networks and corporate IT/enterprise networks, and (ii) industrial networks and the internet network and nodes (including mobile devices).

In the end, huge financial costs could be incurred directly by victims or indirectly through remediation measures after a successful sabotage. For instance, records have that 80% of the UK population depend on five (5) supermarket retailers who hold only four days' worth of stock in their supply chain [50], imagine the consequences of a cyber-attack that effectively disrupts or damage the process control systems. Clearly, the consequences of successful attacks on ICS networks/systems are potentially grave to overlook, and require serious efforts towards mitigation, because ICSs form the building blocks of other critical national infrastructures (energy, gas, transport, aerospace, water, pipeline, communications, and manufacturing). Hence, managerial decisions and actions should emerge from redefined basis and understanding that security now serves the business, and no longer the other way round. They also need to be aware that security risks can only arise if vulnerabilities exist in the company's security architecture.

Cyber-attacks on ICS could be perpetrated in various forms or modes. Authors in [51] recorded four broad classification of attacks targeting ICS, these include; Deception attacks, denial-of-service attacks, replay attacks and covert attacks. Deception attacks aim to compromise the integrity of control packets or quantities and are typically executed by modifying the behaviour of nodes, field equipment, sensors and actuators. An unconventional type of deception attack that could cause prominent damage to ICS is referred to as false data injection attack is presented in [52], this attack mode usually targets static state estimators, and is shown to be capable of evading detection even when designed with limited resources. Similarly, *stealthy deception attacks* against the supervisory control and data acquisition (SCADA) system are analysed, among others, [53]. Similar Stealth attacks against legacy systems and likely counteractive patterns are also considered in [51]. This also works as Data integrity attacks where data could be tainted in the forward or the reverse path in the control flow [54].

Denial of service attacks, on the other hand, targets the compromise of resource availability, for instance, by jamming the communication channel that link ICS devices and nodes. The same approach is termed 'Timing attack' in [54], which works by the saturation of communication network with data packets, causes a snail speed on the network, and possible aa complete shutdown in extreme cases. Replay attacks are executed by hijacking sensors, documenting the readings for a period, and re-echoing such recorded readings to sensors while injecting exogenous signals into the system. Study has shown that such deliberate anomaly could be remedied by inserting random signals unknown to the attacker into the system [55] [54]. A covert attack is also presented, and the effected studied. It follows that a parameterized decoupling structure could allow a covert agent to alter the behaviour of the physical plant while remaining undetected from the original controller [56] .

3.3 ICS Cyber Incidents and Impacts

To properly understand and demonstrate the nature of trends of security incidences against ICSs, we draw from the record of known incidences. For this, the Repository of Industrial Security Incidents (RISI) [57] is used. RISI was started by Eric Byres, Justin Lowe, and David Leversage on the initial

nomenclature called Industrial Security Incidents Database (ISID), which was later modified to RISI. They conceived the idea while working on an academic research project, and purposed to use the database to keep records of incidents cyber security nature that affected (or could have) process control, industrial automation or Supervisory Control and Data Acquisition (SCADA) systems [57]. Being subsequently managed by the Security Incident Organisation (SIO), the RISI databse retains incident records covering the period from 1982 to 2014.

A total of 242 incidents were drawn from RISI covering the period mentioned above. This represents the total of all incidents capture in the data base as at the time of this study. To address the limitation of RISI in covering capturing ICS incidents in the succeeding periods after 2014, we conducted a customised searches for any ICS-related incidents between 2015 and 2018 using google search engine, and found a total of 13 incidents. The metadata description of the incidents found within the scope of time are presented below in Appendix table A. These were combined with the records from RISI ICS incident database [57], and used as the bases for the analysis and discussion in this section. The total of incidents recorded and considered was 255 covering the period 1982 – 2018. Although there are not incidences covering 2015-2018, we believe that the current record provides sufficient numbers of incidents and descriptions enough to derive the insights and trends require in this study. Although this list is by no means exhaustive, we believe that the current sample provides sufficient numbers of incidents and descriptions enough to derive the insights and trends required. The list also gives indication to the extent to which ICSs and related systems are being targeted and the emerging rise in frequency of occurrence. It further consolidates the justification for new and continous responses and mitigation actions against the emerging debilitating circumstance.

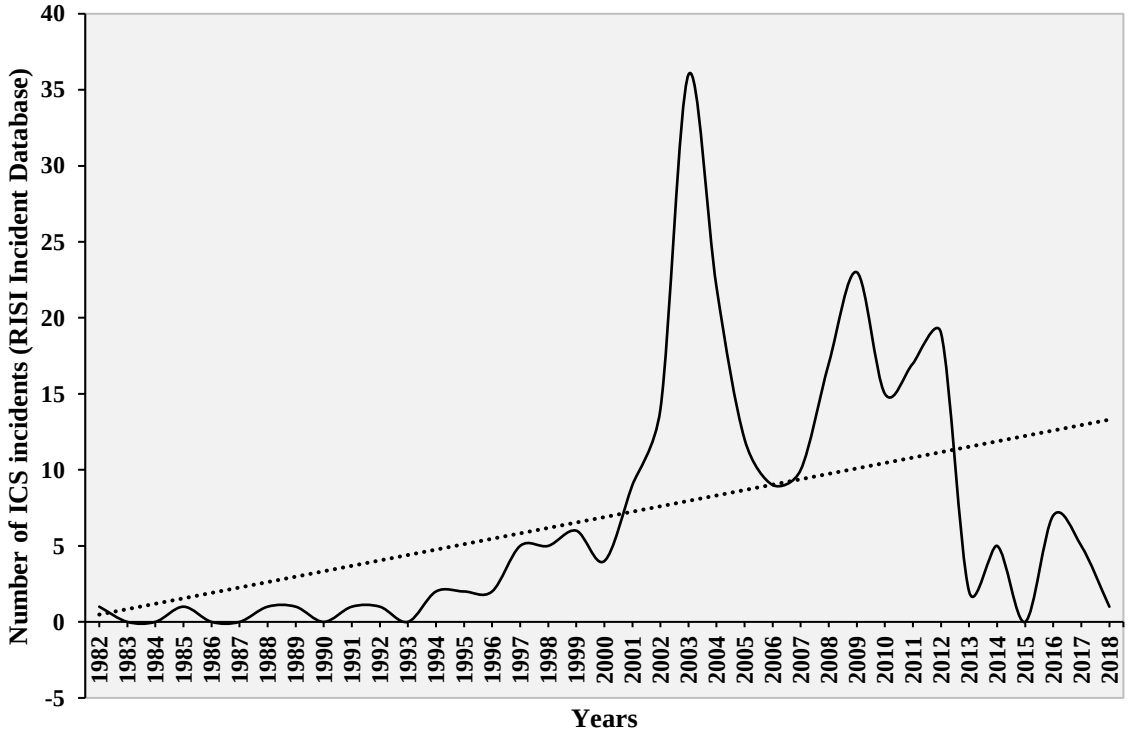

Figure 2: Industrial Control Systems Cyber Incident Representation (Yearly). Analysed from ICS incident records contained in Repository of Industrial Security Incidents (RISI) [57]**.**

Figure 2 shows the trend in the occurrence of security incidences affecting ICS. The first apparent trend to note is that of a steady rise in the numbers of security incident occurences along the period under consideration, especially between 1982 and 2003. Then a steep decline is observed with spikes of incidents happening in some years between 2003 to 2018. The former trend of gradual increase in incidents perhaps represents the period when there were fewer awareness and security solution engagements to control the steady rise. However, as more information and realisation of about the feasibilities of ICS compromise and the damages associated rose to a point that called for more serious

concerns, the response by industries and researchers in discussing and proffering appropriate mitigation solutions could have influenced the decline observed. This also means that if more concerted effforts are engaged, the likelihood is that the trend would continue towards a downward scale.

Again, going by the description of impacts associated to most of the incidents, it appears that as security incidents increase, their impacts on the affected system, and other connected system seem to be getting more significant by the day. These security incidents and their aftermaths demonstrate strongly that that failures and malfunctions in ICS elicited by malicious actors and influences can significantly pose substantial risks; to health and safety of humans, severe impairment to the environment, and economic impacts such as service losses, harm to the industry and by extension a nation's economy, and illegal disclosure of proprietary information. ICS's unique focus on trustworthiness and performance often accounts for its exclusivity in both hardware and software. As seen, these threats and attacks come in varied forms. Jammed or delayed flow of service information through the industrial control networks, hypothetically disrupting industry-critical operations. Illegal changes to service instructions, process commands, or alarm thresholds, capable of damaging, disabling, or worse; shutting down control or service lines or equipment, generating inimical environmental effects, and(or) jeopardizing human life. Wrong information sent to system operators, either in disguise of unauthorized changes, or to influence inappropriate reactions from operators to cause destructive impacts. Modification of control system software or configuration settings, or infection with malware; to cause damage to process/service quality [3].

One striking note is the multi-occurrence of attack patterns targeting and exploiting the human-factor. The people (human element) appear to be a new more attractive targets and easy vectors of attack. Being viewed as the weakest link, most attacks now exploit and rely on human vulnerabilities to accomplish their goals. Social engineering, phisphing, spear-phishing, and improper security administration are quite prominent in the forms of attacks recorded, and their impacts are also grave. For example, the *2016 Prykarpattyaoblenergo incident* [58] that resulted in power cuts in several regions in Ukraine demonstrates how the vulnerability of one employee employee can lead to a very destructive event. Imagine it was a nuclear power plant, surely the consequences would be much worse. We see that infected emails with malicious programmes attached appear to be yielding great effects, despite being considered the least complex type of attack. The successes of this method clearly highlights earlier points of low levels of security knowledge and skills in the ICS domain, with strong security practices and conducts also lacking dangerously, even in the domains with the highest potential risks.This incident and some others in similar fashion continue to emphasise, unfortunately, that the security community is quite behind the bad guys. Security vulnerabilities in ICS are quite multi-pronged, and technology-focused solutions alone cannot assure the best protection. Human and technology components exist in the operational space of ICS, and the solution space need to cater for both ends to gain better security grounds.

In the end, huge financial costs could be incurred directly by victims or indirectly through remediation measures after a successful sabotage. For instance, records have that 80% of the UK population depend on five (5) supermarket retailers who hold only four days' worth of stock in their supply chain [50], imagine the consequences of a cyber-attack that effectively disrupts or damage the supply chain control systems. They would certainly be too severe to turn a blind eye, and require serious efforts towards mitigation. Similarly, ICS and SCADA components and infrastructures form the building blocks of some other national critical infrastructures in, energy, electricity, gas, transport, aerospace, water, pipeline, communications, and manufacturing. Hence, managerial decisions and actions should emerge from a re-defined basis and understanding that security now serves the business, and no longer the other way round. It must be understood that security risks can only arise when vulnerabilities exist in an industrial/organizational security architecture.

4. Securing Industrial Control Systems

In the efforts to address ICS-related security threats, vulnerabilities, and their impacts, several researches have discussed potential techniques to either mitigate or halt completely the incidents and

impacts of cyber-engineered attacks on ICS. In this section, we discuss some of the approaches available in literature.

4.1 Compliance-based Solutions - Standards and Guidelines

Generally, standards, best practices, and guidelines for security usually capture and represent the widely acceptable theoretical and (or) practical thoughts available with reference to specific context and specific value provisioning within certain social and geographical environments and communities. In the context of security; more specifically cyber security, standards emerge as publications accessible freely or paid, publicly or privately that prescribe entities and attributes that provide high assurance of quality in security posture; conforming legal requirements and evolutionary trends. Significant generic roles played by standards, best practices, and guidelines include; Advancing the efficiency and usefulness of key processes, simplifying systems integration and interoperability, aiding easy and meaningful products and methods comparisons, according a means for assessment of products and services, organising the method for new technologies and business models deployment, and promoting economic growth [59].

The quest some of the above interests in ICS brought about the development of guidelines, best practices and standards. The main objectives has been to arrive at prescriptive solution guides for enabling enhanced security assurance in ICS. Consequently, standards very vital roles in improving techniques to security; ICS security across different geographical regions. Among several enablement are; ensuring the incorporation of security-responsive products into a system, decreasing the difficulty of deploying new technologies and business models within and enterprise environment, boosting information exchange among developers, and increasing harmonization among cooperating entities (countries) [59], [60]. However, variations in standards also depicts the corresponding divergent viewpoints from which Information, and ICS securities are being viewed by different organizations, and nations. However, a basic objective shared by all is the desire to achieve a secure system where operations are completely or minimally stalled or interrupted, and security is assured at a reasonably high or acceptable level. This section reviews some of the existing security standards developed for ICS Security, and in Information Security contexts that share applicability to ICS.

ISO/IEC 27002 [61] is a child standard of ISO/IEC 27000 Information Security Standard Series. ENISA's survey report [36] affirms that ISO/IEC 27002 predominant applicability to ICS environment. ISO/IEC 27002 groups security controls by objectives, and follows a best practice guidelines approach for attaining enhanced security. More ICS-specific standards like ISO/IEC 27019:2013 have emerged building upon ISO/IEC 27002, and providing additional information security management system guidelines and recommendations; specifically focusing on energy system.

Defense Information Assurance Certification and Accreditation Process: DIACAP 8510.01 is a US DoD certification and accreditation process for ensuring information security assurance that is also applicable to the ICS domain [60]. The US has also developed technology-specific standards like the Federal Information Processing Standard (FIPS) publication for their defense sector; covering both public and private horizon. A notable technology that has enjoyed provision in this venture include; personal identity verification; in FIPS 201-2 [62]. Other publications in these category include FIPS 199, which deals on information systems security categorisations in the context of the CIA triads, and FIPS 200; which outlines over 17 security-related areas of relevance for information systems, articulating desirable minimum security requirements [60].

There are the National Institute of Standards and Technology (NIST) standards that guide compliance to US Federal Information Security Management Act (FISMA) of 2002. Certain NIST standards provide supplementary guide on the applications of FISMA to ICS [63]. However, NIST SP800-16 [64] specifically focuses on human factors in security, and prescribes the concept of role-based drills as plausible solutions for effective security. Other NIST standards of value to ICS security are spread by naming nomenclatures from SP800-18 to SP800-70, covering disparate areas of security as have been deemed necessary[60].

From the ICS perspective, several standards have been put forward, and a basically categorised into two; cross-industry standards, and industry-specific standards. The former describe standards that could be applied a basic ICS setup irrespective of the field, application, or services involved, while the latter are tailored intentionally to suit specific industries, services, and requirements.

A generic security standard for ICS is the IEC/ISA-62443 [65] published in 2010. Prior to that, the guidelines contained therein were originally published as ISA-199, a name which is still widely acceptable and referenced. ISA-99 captures a wide spectrum security management cycle, grouped under 4 broad classifications; general, policies and procedures, systems, and components. ISA-199 in its standardised nomenclature has been broken down into sub-standards like ISA-62443-2-1 [66] still being reviewed, and ISA-62443-3-2 [67] amongst others to achieve easier target customisation and application.

The UK through it Centre for the Protection of National Infrastructure (CPNI) has also put forward a good practice guideline for the security of IC. The guide covers a wide range of security management areas, from technical factors like secure architecture, to non-technical factors like governance, and human aspects [68], [69]. Industry-specific standards have also been developed in civil aviation [70], and telecommunication [71] amongst others.

A high-level analysis of the standards reviewed in this work; in relations to suitability in the ICS domain does unveil some insights worth noting. In spite of the huge number of security standards out there, very few are applicable to ICS. For instance, of all the NIST information security standards, ICS requirements are only addressed in the FISMA guidelines, and in two others; NIST SP 800-53, SP 800-82. A larger proportion of NIST information security standards do not reasonably come applicable to ICS security objectives due to variations in system operations, service, applications, and protocols. From the ICS security perspective, majority of the publications in use appear to be more of guidelines, only a few have been consolidated into standards (NIST 800-82, NERC 5.21), and even so, the standards are yet widely construed as self-defined regulatory guidelines with non-mandatory compliance assertions and requirements. It is particularly observed that a bulk of the ICS standards reviewed are also noted to emphasize more of technical and process security, and less of people security.

4.2 Applied Security Solutions

Researchers in the ICS security community have discussed different applied techniques and pathways towards achieving security in the ICSE. These methods can be broadly classified into: architectural design, strategy implementation, attack modelling, attack detection, and attack categorisation approaches.

4.2.1 Architectural Design Approaches

These encompass approaches to ICS security explored through the description and(or) establishment of potentially secure design setups (link topologies) - integrating ICS hardware and software into a structured setup to enable a protection capacity. Such design setups are orchestrated to make it difficult for cyber-attacks to happen. Some security concepts that emphasise this approach in literature include: the CockpitCI [72] which discusses a technology-oriented cyber threat awareness improvement approach as a measure towards effective cybersecurity in ICS environments. In [73] a security framework on Cyber-Physical Systems is presented on the bases of threat analysis, taking into consideration; the assessment of risks from four different but related perspectives of the system. These include; assets, threats, vulnerabilities and damages. The security approach emphasizes defense-in-depth (DiD) strategy (i.e. the application of multiple security mechanisms for a same security problem), following a logical hierarchical network structure. This methodology has been further buttressed in [74] and [41]. In [74], to be precise, the concept argued is for defence-in-depth and hierarchical network structure via multiple security mechanism implementations on an ICS/CPS infrastructure. The researchers argue that in control fields, security threats are analysed by means of traditional delays, interference, and fault models, thus, security controls are then accomplished using tolerant controls, distributed estimations, and robust estimations [73], [17]. With such threat potentials, the researchers

advise against focusing solely on security, and argued that "*the significance of safety is even higher than the security. The functional safety and the physical safety must be dependable*" [74]. Thus reaffirming that resilience on CPS/ICS, and controlling cyber-threats requires integrating cyber security knowledge with human interactions, and complex network designs. It must target the maintenance of survivability without the loss of critical functions after intentional cyber-attacks, human errors amongst others, with proper risk analysis covering human, software, and hardware classifications [74].

Other researchers that adopted architectural design approaches include the work in [75], where a trusted computing (TC) architecture is described that combines TC engines with real-time access control infrastructure for system protection. It functions by supporting application platforms for secure distributed applications and enforces the integrity of execution targets, thus preventing the running of untrusted software and also guards against insider threats. While this offers a good solution for checking the integrity of compromised programs and deterring execution, it bears a setback of potentially permitting malicious users to evade detection while exploiting software loopholes. Worse still is the potential for completely altering program execution flows of a trusted inherently insecure program.

A security methodology is proposed [76] that utilizes security patterns (a packaged solution to a recurrent problem) to analyse, build, and evaluate a secure SCADA system. Particularly, the approach employed the study of the general architecture of SCADA systems and the potential attacks inherent. Security patterns are then used as tools to design a secure SCADA system that manages the identified attacks. In [77], a similar approach is described employing the security machineries of a Trusted Platform Module (TPM) to protect the communication in an RPL (Routing protocol) for LLNs (Low-power Lossy Networks). An innovative solution approach that explores Organic Computing (OC) principles is presented in [78]. According to the researchers, the approach can be used to design and implement a potentially secure system/network architecture to meet the emerging cyber threats targeting both IT and OT infrastructure of ICS/CPS. The application of effective key management technology solutions like Public Key Infrastructure (PKI) for securing the smart systems from cyber-breaches is demonstrated in [79], while hierarchical cross-layered design, game-theoretical approach with cross-layered security scheme for securing CPS/ICS is described in [80]. Yet another popular approach for controlling security between associated networks such as production and business networks; is to use multiple firewalls and a DMZ (de-militarized zone). This medium logically enables a middle-tier network for secure data/information transfer, such that devices and their underlying applications operational inside the DMZ assume the places of security agents that guarantees the repression of malicious threats, deterring propagation [81]. The drawback of this is the lack of control over potential internal compromise.

Another security recommendation [82], [5], emphasizes the adoption of the NIST Guide to ICS Security. It highlights incorporating security into network architectures using network segregation practices, as well as disengaging redundant connections to the SCADA network, maintaining a closed-loop (air-gap) as much as possible. Internet connection should only be enabled with the deployment of multiple firewall configurations to sustain the network segregation.

4.2.2 Strategy Implementation Approaches

This includes security establishment concepts and works that address security in ICS through engaging scope analysis, organisational policies, procedures, and technologies, to address security risks. Some works that emphasise this approach: the work on threat analysis and risk assessment that address four elements; assets, threats, vulnerabilities and damages [73]. A strategy involving modelling technique based on weighted Attack and Defense Trees (ADT) structures on ICS/Scada architectures is propose in [83]. The security analysis mechanisms adopted are used to represent cyber attacks through Multi-Terminal Binary Decision Diagrams (MTBDD). MTBDD aids the identification of most probable attack scenarios with respect to probability cost and probability impact. It also helps proffer security mitigation countermeasures for identified security breaches. In [84], a Critical Security Controls Framework is presented aimed at ensuring cyber security by considering and combining the outcomes

of improved malware reporting and gateway monitoring with internal and external security intelligence resources. A similar framework is also discussed in another work [85], this time the basis is on adherence to the security objectives of ICS/CPS.

A "*Big Data Algorithmic*" (data-intensive) approach [12] is presented for defending and safeguarding SCADA system from malware attacks. The method builds bases on the utilization of the data used by control-system designers for making the system robust, and then largely reducing the security and defence problem of control systems or SCADA, alongside the issues of monitoring distributed streaming data. The work proved further that the proposed approach does offer the benefits of scalability and monitoring of complex (large) systems near-behaviours, consequently, decreasing false–alarms potentials. This ultimately exerts security and protection for IT-controlled computing systems. Others in [86] discuss the application of system-theoretic approaches to the real-time security of smart grids which comprises two main process components: contingency analysis (CA) and system monitoring. In [15], a context-aware security approach consisting of three (3) broad level security aspects; sensing security, cyber-security, and control security. The common denominator amongst these works is typically, the conception and implementation of ICS-related security through scope and landscape investigations, and the structuring of policies, procedures, and technologies to meet security threats, vulnerabilities and potential attack patterns.

4.2.3 Attack Detection Approaches

This refer to approaches that typical focuses on uncovering of attacks and breaches from functional and operational faults, behavioural anomalies, malfunction signatures and patterns, and proffering isolation and recovery security and(or) safety controls. A popular technical security concept built around this approach is intrusion detection and prevention. In the ICS network, abnormal conditions would comprise interferences that would require timely recognition and interventions (manually or programme/process automation). Some solutions have taken to the arguable claim that a robust intrusion/anomaly detection system (IADS) is a viable prelude to effective safeguard of ICSs from cyber-attacks. There are quite a bit of researches that have explored this approach with considerable results. Aside from the provision of audit logs and monitoring abilities [46], ICS IDS techniques take advantage of the predictable nature of SCADA traffic, and the fairly static network topology; which could be explored to detect abnormalities, while recognized valid control sequences/codes and unsafe states still make ICS suitable for successful deployment of a signature-based IDS [14]. On this bases, several IDS approaches and schemes have been proposed and validated in either real-life or computer simulated environments to guard against cyber intrusions in ICS/CPS [22], [55], [95]–[97], [87]–[94] .

A study [98] explored the IADS approach of enabling security detection capability through configuration management setup with application whitelisting system (enforcing rigidity of system alterations like reconfigurations, upgrades and specification changes) to lessen attacks that by-pass firewalls and trick users into executing malware. Popular attacks that this measure counters include; binders, web application attacks through cross site scripting, fake/rogue antivirus installations, dynamic link library hijacking, and drive-by downloads. The researcher clarifies that most of these attacks could be easily employed by script kiddies, or unsophisticated individuals who simply download and run executable files from the internet.

In [99], a System Theoretical Accident Model and Process (STAMP) approach to safety and security, which views systems as dynamic entities with safety and security control issues. STAMP methodology is based on three supports: (i) safety control structure, (ii) safety constraint, and (iii) process model. A Model-based approach to self-protection is presented in [100], which employs autonomic computing technology. It is used to monitor system performance, and proactive estimation of imminent attacks for a given system model of a physical infrastructure. In [101], a model that integrated various techniques for detecting attacks in critical infrastructures and enforcement of security policies to minimise attacks is presented. The model considers the interposition of an attack detection agent (ADA) between the hardware and the server systems; for the gains of overcoming the limitations of an existing Security Enforcement Module (SEM), and dealing with the attacks. Using validated test scenarios, the model is

seen to be reasonably effective; as it is able to detect the compromise of a system during runtime state validation of the system, and/or when the attacker uses the compromised system to generate attacks such as flooding the critical infrastructure network

In [102] generic hierarchical model for performance analysis of intrusion detection techniques as applied to a cyber-physical system ICS/CPS consisting of mobile nodes with navigation, manipulation, sensing and actuating capability. The intrusion detection techniques developed for malicious discovery of ICS/CPS directed attacks include; positional discontinuity and enviro-consistency, with propositions of potentially optimal design settings under which the reliability of the ICS/CPS may be maximized. Similarly, security is explored through a coupled design framework that adopts the cyber configuration policy of Intrusion Detection Systems (IDSs) and the robust control of dynamical system [103]. The approach uses design algorithms based on value iteration methods and linear matrix inequalities for computing the optimal cyber security policy and control laws. Researchers in [104], [105] explored modelling the causal relationship between devices in a cyber-physical system using a Bayesian Networks and a resultant expansion called 'causal event graphs', used to model deterministic signatures which can be used by an intrusion detection system to classify events. In [106], a unified modelling framework and an advanced detection procedure requiring only local network knowledge for implementation is presented. The modelling framework captures details about system properties like network components malfunction and measurements corruption, and uses same to guide the detection of cyberattacks. Researchers in [46] recommended the adoption of the NIST Guide to ICS Security, with specific highlights security-oriented network architectures via network segregation practices, as well as disengaging redundant connections, and maintaining a closed-loop (air-gap) as much as possible.

4.2.4 Protocol Hardening Approaches

This refers to the concepts of incorporating security features into existing ICS protocol stacks and functionality to enable some level of security enhancement. Some works have explored this approach with some considerable results. For example, while attempting to address identified potential attack instances against the DNP3 protocol in ICS networks, a conceptual DNPSec security technique [107], which supports confidentiality, integrity, and authenticity is presented, with appropriate model validation as a future work. Similarly, the security weaknesses of Modbus TCP and IEC 61850 is illustrated [92] with emphasis on defective or missing cryptographic protection, and memory corruption vulnerabilities. Given that both protocols are deployed in C/C++ language, they are found to be prune to multiple protocol-specific and generic memory corruptions. Other Modbus attack forms like '*Pure-data*' permit overwriting non-control data, contributing to the actual computations done by control applications, which of course pave ways for further compound attacks on physical equipment and processes. The authors in [108] proffered a potential solution (adding security capabilities for integrity, authentication, and anti-replay protection) that hinges success on the effective preservation of secrecy of shared keys.

Still focusing on protocol security, another methodology for managing memory corruption attacks on Modbus ICS [109] is also presented. It involved imposing logical limitations between hypothetically hostile data and safe data in secured processes. It works by encrypting all input data using random keys, with the encrypted data stored in primary memory and decrypted following the least privilege principle just before it is processed by the CPU. It is emphasised that this measure ultimately upsets the precision with which adversaries can compromise control data and pure data; guarding against the likes of code injection, arc injection attacks, and lessening the challenges imposed by the ascendency of mitigation techniques. A set of hypothetically demonstrated attacks on PROFINET IO and PROFIsafe [110] and [111], indicate the potentials for hijacking PROFINET/PROFIsafe node while evading detection from peers. A formal procedure for assessing the security of multi-layered SCADA protocols in the context of ModbusTCP is presented [94]. Similar solution path has been charted by other researchers [95]; proposing a lifelike framework that supports formal representation of control components and processes under control. They further developed an error identification algorithm which explores accurate model

to bind cyber security relevant components with process control elements. It works by identifying process variances, and maps same; either to a conventional fault source or to a component under cyber-attack.

4.2.5 Attack Modelling Approaches

This refers to solution concepts and works that explore ICS security through the replication of cyber-attack events in simulation, emulation, or real environments. It involves the study of vulnerability patterns, direct and cascading effects and impacts of exploiting the vulnerabilities, and using observed and evaluated results to bring about effective security solutions.

Works within this areas incoude; a self-contained control-theoretic approach to cyber-physical security [51] is also proposed. The concept was a build-up to an earlier work [55] that took abstraction from classic works on geometric control theory [112], [113], including deterministic static detection problem covered in [114], and the prototypical deception and denial of service, stealth [115], self-motivated false-data injection [116], replay attacks [117], and covert attacks [52] as exceptional cases. The resulting unified modelling framework explores the modelling of cyber-physical systems under attack as descriptor systems subject to unknown inputs; modifying the state and the measurements. The solution proposed seem sufficiently generic to suite numerous attack scenarios. Accoding to the researchers, the modelling scheme also allows for a rigorous study of the detectability and identifiability of attacks, a broad analysis of attack effects on affected system, and the design of monitors and attack remediation schemes, with appropriate and coordinated attacks case study for validation [51]. In [118], a framework for modelling the security of a cyber–physical systems is described in which the adversarial behaviour is controlled by a threat model that captures – in a unified manner – the cyber aspects (with discrete values) and the physical aspects (with continuous values) of the cyber–physical system. Researchers in [119] worked on the modelling and analysis of vulnerability of information and communication (cyber) network using concepts of discovery, access, feasibility, communication speed and detection of threat. Similarly, researchers [120] used simulation modelling approach for representing computer networks and intrusion detection systems (IDS) to efficiently mimic cyber-attack scenarios and detection potentials. In [121], a Hybrid Attack Graph (HAG) mechanism is used for modelling both the physical and cyber components of attacks. The HAG provides insight into potential attack vectors, and potential points of security improvements. In [122], a test-bed for Secure and Robust SCADA Systems is described. The authors argued that a better understanding of how to safeguard SCADA systems could only be achievable via adequate test-bed approach for vulnerability assessment and development of appropriate security mechanisms.

4.2.6 Attack Categorisation Approaches

This delineates the approach in some literatures exploring security enablement through the classification of cyber-attacks based on exploit modes for attacking ICS systems, and engaging specific controls to meet specific attack modes. For example, the works in [123], [112] discuss concepts that project categorisations using taxonomy of cross-domain attack patterns. In [124], [103], development of defensive solutions to guard against the excessive flooding of device controllers and systems with invalid traffic data. In [125], a jamming attack is discussed, which involves using game theoretical framework to study the interactive decision making process of attacks, and effectively congestion communication channels, to slow or bar communication. [126] explore a security solution through the study of the performance of Stealthy Deception Attacks from a systems perspective. [127] discusses similar solution but focused on Man in the middle attack – the interception of correct messages, and sending of false messages to a devices or operator.[128] explores security against the access and interpretation of encrypted or secure information using compromised-key attacks. Researcher in [129] proposed a new detection scheme against replay attacks based on prior control system solutions, while security solution against Eavesdropping – the listening in on information communicated by cyber-physical systems is presented in [130].

4.2.7 Analysis

As it appears, when it come applying tailored approaches to secure ICSs from cyber-related attacks and compromises, several approaches may be adopted to achieve specific security objectives and capacities within the system. The application of secure design architecture provides a way of establishing a multi-layered security capacity enabled in system and network components, to toughen the process attacker have to go through, and potentially lessening the success rates in attempted compromise events. This technique reflects a proactive security approach geared to make it difficult for attacks to happen in the first place. This notional path towards establishing or enhancing security in ICS seem to enjoy wide acceptance judging by growing researches in the area. And of course, common standards such as NIST SP 800-82 Rev 2 [37] have also sign-off on this approach. It is quite helpful to be guided by such standards which emphasize the adoption of the NIST Guide to ICS Security. It highlights incorporating security into network architectures using network segregation practices, as well as disengaging redundant connections to the SCADA network, maintaining a closed-loop (air-gap) as much as possible. Internet connection should only be enabled with the deployment of multiple firewall configurations to sustain the network segregation.

Implementing defense-in-depth is with suggestive implementation approaches including real time access control mechanisms using firewalls, Demilitarised-zones (DMZs), trusted computing, and public key infrastructure are some security features that come useful in this approach. This theory of applying defense-in-depth strategy for the security of ICS is also supported in a US-government security report [131] as part of a holistic measure against ICS cyber-security. The approach appears to be closest towards achieving the commonly advocated security-by-design principle from the network perspective, a measure believed to retain the capacities to subvert growing security threats and vulnerabilities in evolving security landscape. Security-by-design technique can proffer a more realistic, robust cyber security in industrial networks; making way for better visibility, integration, performance, and security in all subdivisions within the enterprise networks. The application of strategy implementation is also a good approach proffered by researchers, although not much as compared to the sign-offs on secure architecture approach. The emphasis on security scope and policy analysis to drive the adoption of technical and procedural controls puts the approach more on the proactive side of security, and helps to ensure that security controls exist or are implemented from a good understanding of the capacity required. It also feeds the reactive part when cyber compromises occur and appropriate security countermeasures are required. Attack trees, defense trees, data analytics and context-awareness analysis are concepts that have been commonly considered in this approach.

Attack detection, especially via the use of intrusion detection and prevention system is also both a proactive and a reactive security measure chiefly focused detecting attacks and compromises when they happen in order to engage appropriate security countermeasures to forestall the inherent, and perhaps future similar occurrences. There appears to be a wide acknowledgement and exploration of this approach in literatures. This often goes or works well with the attack categorisations approach However, despite the efforts and progresses made in the demonstration and use of intrusion/anomaly detection approaches for ensuring effective security in ICS, open questions still abound that seek to strengthen further the arguments as to the effectiveness of IDS for ICS cyber-security. These could be attributed to unclear justifications from some of the existing IDS approaches, unclear or omitted implementation guidelines, limitations, and simulation results [14]. These give rise to unresolved issues like the analysis of IDS performance during alarm flooding caused by anomalous conditions. Typically in ICS platform like manufacturing, as earlier noted, anomalous situations would encompass a range of process disruptions - minor or major, in which recognitions and interventions would be required by operations/floor personnel to correct problems the control systems is unable to handle. A complementary challenge also relates to the precise identification of the sources for process misbehaviours to allow for appropriate remediation measures [14]. Notwithstanding, intrusion and anomaly detection systems have been shown to be implementable at the network and/or host layers of ICS infrastructures. In an example case study [93], an anomaly detection model for nuclear power plants was used to investigate the detection of potential attacks that attempt to transmit erroneous data to HMIs

from a field device. The demonstration substantiates a later work [10] that asserts the ability to extend anomaly detection models to the SCADA environment.

ICS protocol hardening contributes security by introducing or enabling traditional security features such as encryption unto proprietary communication protocols which do not have in-built security features. The approach is typically aimed at enforcing integrity, authentication and anti-replay protections against ICS components and network. This approach is often implemented along with the implementation of secure architecture. While this approach of hardening protocols may be useful, effectiveness are often affected by low processing power of the ICS devices, so that not much of the state-of-the-art security mechanism can be appropriately added to boost security posture. This makes that protocol hardening alone may not provide or assure the desired kind of security for ICSs. Ensuring effective security via attack modelling also brings in its unique kind of value, given the emphasis on the replication, study, and understanding of the nature of potential attacks, and analysis of their impacts. Thus, bringing about the implementation of controls from more realistic threats, vulnerabilities, and impact evaluations. This method also tries to address the typical challenge of a lack of sufficient prior data about cyber incidents upon which control decision can be made. With modelling approach, attack detection, strategy implementation and secure architecture approaches often set in, and the opportunity to explore or investigate their effectiveness on ICS is enabled. As it appears, not one of the mentioned security approaches can exists independently. These approaches more highly emphasise technical security capacities, hence, each of the approaches is often actualised or complemented by one or more of the other. This indicates that technical solutions are quite instrumental to ensuring security on ICSs, and in fact, appear to be the most explored approaches for that purpose in the industrial environment.

5. ICS Security Fissures and Recommendations

A careful evaluation and characterisation of the security approaches reviewed in relations to the initial reviews of inherent ICS cyber security concepts, principles, threats, vulnerabilities, incidents and impacts, surely brings to light the absence of certain elements which can contribute to more coverage of security in the ICS domain.

5.1 Weakness of a One-Dimension Security Approach

Some approaches have followed theoretic concepts, while others have adopted and used experimental test cases and environments as viable lifelines in the search for security relevance for ICS/CPS. This again is observed to bear greater focus on SCADA systems; being that part of the larger system that exerts control and managements of other ICS-system parts. Particularly noted, is that a bulk of the security approaches reviewed clearly adopt technological dimensions for attainment of cybersecurity, while most favour one-directional technological mechanism and(or) enhancements, very few have seen and emphasise the integration of multiple technology solutions. The assumption is that; technology is about the most important constituent of industrial control system infrastructure. Although the significance of the technology security propositions have been recognised and well-applauded [3], [5], [38], [132], the assumptions and exertions of greatest significance has overtime; proved to be farfetched going by the attack patterns and number of incidents emerging. And to add, technical security solutions should think of including internet-facing security capabilities since most of the evolving attacks are reported emanating from and via the internet. This way, the vulnerability landscape of ICSs can be covered in relations to solution development.

5.2 Mis-alignment of Security Management Strategy

This is a succeeding factor to the previous phenomenon. Careful study of the details surrounding reviewed ICS cyber incidents revealed that their successes have been made possible by the actions and (or) inactions of human-elements within and (or) outside the system. Nonetheless, most cyber security expert do not consider humans to be part of the ICS system, and most unfortunately; the weakest part [133], [134], [135] due . Hence, solutions (strategies and models) have however not adequately provisioned protective capacities for this frailest entity.

A closer look at the trending attack modes and patterns reveal quite remarkable dynamics. Much of the recurrent cyber-attack strategies and mechanisms (spear-phishing, social engineering, compromise of domain controllers, attacks on exposed servers, attack on ICS clients, Session hijacking, errors and omissions in the firewalls configurations, forged Internet Protocol addresses, and sneaker net techniques) evidently have one thing in common; placing humans as the primary or first-point targets for enabling the penetration and actualization of malicious deeds within the digital system, with the effectiveness of malicious objectives largely depending on the behavioural/operational responses of the human elements. Cyber assailants exploit human weaknesses in knowledge, skills, discipline and technical-know-how; to further their spiteful objectives. So while security efforts are busy protecting technology (indicated as defence outlook B in Figure 3), violence efforts are busy attacking people (indicated as attack outlook A in Figure 3). Clearly a misplacement of focus for effective cyber security. A point that has not been properly conceived by ICS owners is that this frailest part; the workforce; is the potentially the strongest security asset of an ICS structure, not its technology nor policies; but in its workforce – people-constituents [136]. The workforce are key stakeholders in an organization's business of attaining cyber security. They are active contributors in the day-to-day activities and operations, and respond the security requirements that reflect an organization's attitude, value, and target for efficiency.

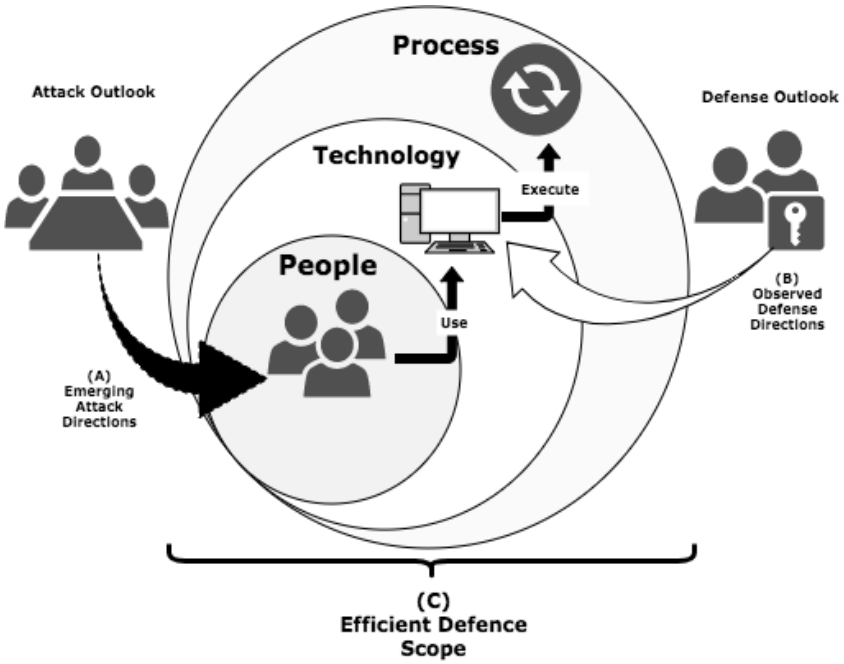

Figure 3: ICS Security Trends (Attack and Defense Outlook)

Accordingly, as the attack gaze has changed, the security gaze and concepts require change as well; if cyber security assurance is to be achieved. Every typical ICS infrastructure consists of people, processes, and technologies, and all of these components must be catered for adequately in any effective security solution of strategy (indicated as efficient defence scope C in Figure 3). It is observed evidently, that; despite the surplus of technology solutions, cyber-attacks against ICSs continue to emerge at alarming rates.

5.2 Few Generic Applied Solutions

Noticeably, most of the security propositions are industry/domain-specific; covering specific areas like power and energy generation and distribution, smart grid, and fluid distributions. Contextually, the application in one is constructed such that it is potentially inappropriate for another due to variations in systems and structural designs, and service objectives. It is observed however; that certain areas currently witnessing huge attack hits like manufacturing; have not enjoyed adequate attention overtime. Given that there are basic infrastructure (devices, protocols, and services) that most if not all of these

different control system areas share, it is appropriate to have more generic solutions and standards that would offer robust solutions irrespective of the field of control system applications.

6. Conclusion

The cyber security uncertainties in the industrial control system environment are pretty much, and as developments continue to advance, it is feared that these challenges will continue to grow. Generally, these threats are persistent and evolving such that a purportedly viable countermeasure yesterday does not necessary reflect same today, or even tomorrow. Attackers have remained consistent in refining old ways and devising new ones for assaulting their targets. The only way to effectively respond to these is to have solutions that follow similar evolutionary pattern as the problem trends. Cyber security measures that would embrace constant progression in response to changes in the threat, vulnerabilities, attacks, and impact domains. It would imply seeking long-term solutions and recurrently fine-tuning them accordingly; to avoid the pitfalls of transitory security by decision managers who rely on one-off purportedly bullet-proof solutions. Unfortunately, if they ever did, such do no exist anymore in the cyber security domain.

Given the foregoing, assuming a biased solution in favour of any of the ICS functional constituents can hardly yield an all-encompassing security as desired. For example, technical security solutions alone cannot offer the best solution. Even in the technical solutions, several approaches need to be integrated and combined to form a formidable security force against cyber instrusion and compromises. Technology is evidently no solution to human incompetency and (or) inaccuracies. Thus, an effective security solution for ICS requires harmonizing specific constituent solutions into a singular, robust, anticipatory security setup. Security, cyber security by its nature must be viewed with levels of uncertainties that aptly describe the nature of the environment.

Effective cyber security requires effective management from an organization standpoint that captures solutions reaching out to all entities that make up a functional ICS. For the envisioned security to be achieved in any ICS-driven environment, operational/functional security objectives need to be well articulated in line with business needs, adequate security policies established that enforce defined objectives, strong security and implementation strategy, audit and assessment plans outlined. These have to be done with the full understanding that targeted security vulnerabilities and risks being guarded against are such that are distributed across ICS operational entities; people, process, and technology. Cyber security is a continuous process that does not end with a good implementations of technology solutions. Operational security processes need to be constantly monitored and reviewed in the light of emerging trends. Human actors in the system also need to be monitored and upgraded in terms of security knowledge and skills in relations to evolutionary security trends, standards, certifications and best practices.

Greater emphasis are being laid on efficient services and customer satisfaction for which cyber security is turning a condition for purchase - a precondition for engaging in business. Customers expect industrial owner to take up responsibility for defending their services and products, and to engage every practicable means for preserving productivity, personality, and functionality. Thus, industrial critical infrastructure protection require creating sustainable modifications to a whole industrial system's structure to simultaneously advance three protection qualities; safety, security and resilience. These should be supported with relevant or associated ancilliary security principles such as timeliness, veracity, authenticity, non-repudiations, and reliability. Perceptibly, this call for improved scope would typically drive the harmonization of people, process and technology security essentials as means to an end. This approach is aimed at enabling the move towards a more matured, assured cyber security posture, where ICS are being operated with relative security and with minimal potentials for unplanned, unforeseen, uncontrollable significant damage or interruptions. The very pertinent objectives remains the attainment of sufficient resistance and resilience to withstand failures influence by malicious intentional or unintentional cyber action.

There are also needs for tailored principles, best practices, and taxonomies for measureable cyber security, and to determine whether these different principles and practices are hinged on the infrastructure or types of control systems. Determining how the composition of ICS components lead to the composition of system assurance properties; is as desirable as the development of cyber security metrics and models for quantifying the impacts of potential cyber-attacks upon critical equipment, and the physical environment. The improvement in awareness, development, and evaluation methods for ICS workforce cyber security knowledge and skill especially for the direct operators of the systems. In the end, the security approach that can be effective would most likely draw from a combination of compliance to appropriate security policy, guideline and standards, and a tailored implementation of technical, process, and human-factor security solutions.

References

[1] E. Van Der Zwan, "Security of Industrial Control Systems, What to Look For," *ISACA J. Online*, vol. 4, no. 10, pp. 1–9, 2010.

[2] J. F. Brenner, "Eyes wide shut: The growing threat of cyber attacks on industrial control systems," *Bull. At. Sci.*, vol. 69, p. 15, 2013.

[3] S. Radack, "Protecting Industrial Control Systems - Key Components of Our Nations Critical Infrastructures," *ITL Bulletin*, no. August, Gaithersburg, Maryland, pp. 1–7, Aug-2011.

[4] S. Rautmare, "SCADA System Security: Challenges and Recommendations," in *2011 Annual IEEE India Conference (INDICON)*, 2011, pp. 1–4.

[5] T. Lu *et al.*, "Cyber-Physical Security for Industrial Control Systems Based on Wireless Sensor Networks," *Downloads.Hindawi.Com*, vol. 2014, 2014.

[6] ChecPoint, "Protecting Industrial Control Systems," San Carlos - Califonia, 2015.

[7] Citicus, "Risk Management for Industrial Control System," *Citicus ICS*, 2015. [Online]. Available: http://www.citicus.com/citicus_ics_characteristics.asp. [Accessed: 12-Mar-2016].

[8] U. P. D. Ani, H. (Mary) He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, 2017.

[9] Siemens, "Securing Industrial Control Systems. The Challenge and Common-sense," Germany, 2018.

[10] R. D. Larkin, J. Lopez Jr., J. W. Butts, and M. R. Grimaila, "Evaluation of Security Solutions in the SCADA Environment," *Data Base Adv. Inf. Syst.*, vol. 45, no. 1, pp. 38–53, 2014.

[11] A. Cardenas, A. Saurabh, S. Bruno, G. Annarita, P. Adrian, and S. Shankar, "Challenges for Securing Cyber Physical Systems," in *Workshop on Future Directions in Cyber-physical Systems Security*, 2009.

[12] R. K. Shyamasundar, "Security and Protection of SCADA : A Bigdata Algorithmic Approach," in *Proceedings of the 6th International Conference on Security of Information and Networks*, 2013, pp. 20–27.

[13] D. Gollmann, *Computer Security*, Third Edit. West Sussex: John Wiley & Sons, Ltd, 2011.

[14] M. Krotofil and D. Gollmann, "Industrial control systems security: What is happening?," *2013 11th IEEE Int. Conf. Ind. Informatics*, pp. 664–669, 2013.

[15] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Security Issues and Challenges for Cyber Physical System," in *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, 2010, pp. 733–738.

[16] D. Work, A. Bayen, and Q. Jacobson, "Automotive Cyber Physical Systems in the Context of Human Mobility," in *National Workshop on High-Confidence Automotive Cyber-Physical Systems*, 2008, pp. 3–5.

[17] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Comput. Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[18] G. Pender-Bey, "The Parkerian Hexad: The CIA Expanded," Lewis University, 2012.

[19] W. Stallings, *Cryptography and network security: principles and practice*, 5th Editio. Upper Saddle River, NY: Pearson Education, Inc., publishing as Prentice Hall. l, 2010.

[20] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proceedings - International Conference on Distributed Computing Systems*, 2008, pp. 495–500.

[21] D. Gollmann, "Veracity, Plausibility, and Reputation," in *Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems, Volume 7322 of the series Lecture Notes in Computer Science*, I. Askoxylakis, H. C. Pöhls, and J. Posegga, Eds. Egham, UK: Springer Berlin Heidelberg, 2012, pp. 20–28.

[22] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing*,

iThings/CPSCom 2011, 2011, pp. 380–388.
[23] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," *2009 IEEE/PES Power Syst. Conf. Expo. PSCE 2009*, pp. 1–8, 2009.
[24] L. Wu and G. Kaiser, "FARE: A framework for benchmarking reliability of cyber-physical systems," *9th Annu. Conf. Long Isl. Syst. Appl. Technol. LISAT 2013*, 2013.
[25] L. Wu and G. Kaiser, "An Autonomic Reliability Improvement System for Cyber-Physical Systems," *2012 IEEE 14th Int. Symp. High-Assurance Syst. Eng.*, pp. 56–61, 2012.
[26] R. Mitchell and I.-R. Chen, "Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems," *IEEE Trans. Reliab.*, vol. 62, no. 1, pp. 199–210, 2013.
[27] M. Rungger and P. Tabuada, "A Notion of Robustness for Cyber-Physical Systems," pp. 1–27, 2013.
[28] M. Rungger and P. Tabuada, "Abstracting and refining robustness for cyber-physical systems," *Proc. 17th Int. Conf. Hybrid Syst. Comput. Control - HSCC '14*, pp. 223–232, 2014.
[29] P. Tabuada, S. Y. Caliskan, M. Rungger, and R. Majumdar, "Towards Robustness for Cyber-Physical Systems.," *IEEE Trans. Automat. Contr.*, vol. 59, no. 12, pp. 3151–3163, 2014.
[30] H. a. Boyes, "Trustworthy cyber-physical systems - a review," *8th IET Int. Syst. Saf. Conf. Inc. Cyber Secur. Conf. 2013*, pp. 1–8, 2013.
[31] L. Chen, "The Model and Method of Trustworthiness Level Evaluation for Software Product," no. Icnc, pp. 709–715, 2010.
[32] L. Zhang, Y. Zhou, Y. Chen, M. Zhang, and J. Zhang, "Stability of Software Trustworthiness Measurements Models," *2013 IEEE Seventh Int. Conf. Softw. Secur. Reliab. Companion*, pp. 219–224, 2013.
[33] R. W. Anwar and S. Ali, "Trust Based Secure Cyber Physical Systems," in *Proceedings of the Workshop on Trustworthy Cyber-Physical Systems run on September 3, 2012 in conjunction with CONCUR 2012.*, 2012, no. August, pp. 1–10.
[34] B. Stelte and G. D. Rodosek, "Assuring trustworthiness of sensor data for cyber-physical systems," *Integr. Netw. Manag. (IM 2013), 2013 IFIP/IEEE Int. Symp.*, pp. 395–402, 2013.
[35] L.-A. Tang, X. Yu, S. Kim, J. Han, C.-C. Hung, and W.-C. Peng, "Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems," *2010 IEEE Int. Conf. Data Min.*, pp. 1079–1084, 2010.
[36] ENISA, "Protecting Industrial Control Systems Recommendations for Europe and Member States," Greece, 2011.
[37] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security - NIST.SP.800-82r2," 2015.
[38] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastruct. Prot.*, vol. 8, pp. 53–66, 2015.
[39] J. Weiss, *Protecting industrial control systems from electronic threats*. New York: Momentum Press, 2010.
[40] A. Gervais, "Security Analysis of Industrial Control Systems," KTH Stockholm and Aalto University, 2012.
[41] E. Byres, D. Leversage, and N. Kube, "Security incidents and trends in SCADA and process industries," *Ind. Ethernet B.*, vol. 39, no. May, pp. 12--20, 2007.
[42] Symantec, "Triton: New Malware Threatens Industrial Safety Systems | Symantec Blogs." Symantec, 2017.
[43] M. Austin, "Sophisticated 'Triton' malware shuts down industrial plant in hacker attack." Designtechnica Corporation, p. Digital Trends Website (Computing), 2017.
[44] S. Gibbs, "Triton: hackers take out safety systems in 'watershed' attack on energy plant | Technology | The Guardian," *The Guardian News (Online)*, p. Technology News page, 15-Dec-2017.
[45] IBM, "A Strategic Approach to Protecting SCADA and Process Control Systems," Atlanta, 2007.
[46] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ.*, pp. 1–157, 2011.
[47] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, Oct. 2006.
[48] W. T. Shaw, "Identifying Cybersecurity Vulnerabilities," in *Cybersecurity for SCADA Systems*, Illustrate., S. Hill, A. Hensley, and T. Quinn, Eds. Tulsa, Oklahoma: Penn Well Corporation, 2006, p. 261.
[49] Kaspersky Lab ICS CERT, "Threat Landscape for Industrial Automation Systems in H1 2017," Kaspersky Lab, 2017.
[50] R. Piggin, "Cyber security and Critical National Infrastructure," no. 1.
[51] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-Theoretic Methods for Cyberphysical Security:

Geometric Principles for Optimal Cross-Layer Resilient Control Systems," *IEEE Control Syst.*, vol. 35, no. 1, pp. 110–127, 2015.
[52] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, pp. 1–33, 2011.
[53] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *49th IEEE Conference on Decision and Control (CDC)*, 2010, pp. 5991–5998.
[54] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment," *J. Adv. Res.*, vol. 5, pp. 481–489, 2014.
[55] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack Detection and Identi fi cation in Cyber-Physical Systems," *IEEE Trans. Automat. Contr.*, vol. 58, no. 11, pp. 2715–2729, 2013.
[56] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," in *IFAC Proceedings Volumes (IFAC-PapersOnline)*, 2011, vol. 18, pp. 90–95.
[57] Exida, "RISI Online Incident Database," *Online Database*, 2015. [Online]. Available: http://www.risidata.com/Database. [Accessed: 17-Aug-2018].
[58] D. BISSON, "BlackEnergy Malware Caused Ukrainian Power Outage, Confirms Researchers," *Tripwire Online Magazine*, Jan-2016.
[59] S. Purser, "Standards for Cyber Security," *Best Pract. Comput. Netw. Def. Incid. Detect. Response*, pp. 97–106, 2014.
[60] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, 2015.
[61] ISO/IEC 27002, "International Organization for Standardization; Information Technology – Security Techniques – Code," Geneva, 2005.
[62] NIST, "FIPS PUB - Personal Identity Verification (PIV) of Federal Employees and Contractors," 2013.
[63] FISMA, "Industrial Control System Security," Gaithersburg, Maryland, 2014.
[64] S. I. Zafra, Dorothea E. de Pitcher *et al.*, *Information Technology Security Training Requirements: A Role- and Performance-based Model*. Gaithersburg, Maryland: Information Technology Laboratory-National Institute of Standards and Technology, 1998.
[65] IEC, "(IEC/TS 62443- 1-1) - Industrial Communication Networks - Network and System Security – Part 1-1: Terminology, Concepts and Models," Geneva- Switzerland, 2009.
[66] ISA, "Security for Industrial Automation and Control Systems, Part 2-1: Industrial Automation and Control System Security Management System (ISA-99 Draft 7, Edit 5)," North Carolina, 2015.
[67] ISA, "Security for industrial automation and control systems Part 3-2: Security risk assessment and system design (ISA-62443-3-2, Draft 6, Edit 2)," North Carolina, 2015.
[68] CPNI, "Good Practice Guide Process Control and Scada Security Guide 2 . Implement Secure Architecture," London, 2008.
[69] CPNI, "Good Practice Guide Process Control and SCADA Security," London, 2008.
[70] CPNI, "Cyber Security in Civil Aviation," London, 2012.
[71] CPNI, "RESILIENCE IN CONVERGED NETWORKS Resilience in Converged Networks :," London, 2009.
[72] T. Cruz *et al.*, "Improving cyber-security awareness on Industrial Control Systems : the CockpitCI approach," in *13th European Conference on Cyber Warfare and Security Th University U i it of f Piraeus Pi*, 2014, pp. 59–69.
[73] T. Lu, B. Xu, X. Guo, L. Zhao, and F. Xie, "A New Multilevel Framework for Cyber-Physical System Security," in *First International Workshop on the Swarm at the Edge of the Cloud (SEC'13 @ ESWeek)*, 2013, pp. 2–3.
[74] P. Dong, Y. Han, X. Guo, and F. Xie, "A Systematic Review of Studies on Cyber Physical System Security," vol. 9, no. 1, pp. 155–164, 2015.
[75] M. Burmester, "A trusted computing architecture for critical infrastructure protection," *Iisa 2013*, pp. 1–6, 2013.
[76] E. B. Fernandez, J. Wu, M. M. Larrondo-Petrie, and Y. Shao, "On building secure SCADA systems using security patterns," *Proc. 5th Annu. Work. Cyber Secur. Inf. Intell. Res. Cyber Secur. Inf. Intell. Challenges Strateg. - CSIIRW '09*, p. 17, 2009.
[77] S. Seeber, A. Sehgal, B. Stelte, G. D. Rodosek, and J. Schonwalder, "Towards a trust computing architecture for RPL in Cyber Physical Systems," in *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, 2013, pp. 134–137.
[78] J. Haehner *et al.*, "A Concept for Securing Cyber-Physical Systems with Organic Computing Techniques," in *Architecture of Computing Systems (ARCS), Proceedings of 2013 26th International Conference on*, 2013, vol. 9, p. 1.
[79] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*,

vol. 1, no. 1, pp. 99–107, 2010.
[80] Q. Zhu, C. Rieger, and T. Başar, “A hierarchical security architecture for cyber-physical systems,” in *Proceedings - ISRCS 2011: 4th International Symposium on Resilient Control Systems*, 2011, pp. 15–20.
[81] Honeywell, “Cyber Security in Manufacturing & Production,” 2011.
[82] R. Shbib, S. Zhou, and K. Alkadhimi, “SCADA system security, complexity, and security proof,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7719 LNCS, pp. 405–410, 2013.
[83] A. Bobbio, L. Egidi, R. Terruggia, E. Ciancamerla, and M. Minichino, “Weighted attack trees for the cybersecurity analysis of SCADA systems,” in *3rd International Defense and Homeland Security Simulation Workshop, DHSS 2013, Held at the International Multidisciplinary Modeling and Simulation Multiconference, I3M 2013*, 2013, pp. 33–40.
[84] S. Northcutt, “Breaches Happen : Be Prepared,” 2014.
[85] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, “Towards a Framework for Assuring Cyber Physical System Security,” vol. 9, no. 3, pp. 25–40, 2015.
[86] B. Y. Mo *et al.*, “Cyber – Physical Security of a Smart Grid Infrastructure,” *Proc. IEEE*, vol. 100, no. 1, pp. 1–15, 2011.
[87] M. Naedele and O. Biderbost, “Human-assisted intrusion detection for process control systems,” *Proc. 2nd Int. Conf. Appl. Cryptogr. Netw. Secur.*, pp. 216–225, 2004.
[88] I. N. Fovino, M. Masera, M. Guglielmi, A. Carcano, and A. Trombetta, “Distributed intrusion detection system for SCADA protocols,” in *IFIP Advances in Information and Communication Technology*, vol. 342 AICT, T. Moore and S. Shenoi, Eds. Springer, IFIP Publications, 2010, pp. 95–110.
[89] D. Hadžiosmanović, L. Simionato, D. Bolzoni, E. Zambon, and S. Etalle, “N-gram against the machine: On the feasibility of the N-gram network analysis for binary protocols,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7462 LNCS, pp. 354–373, 2012.
[90] D. Hadžiosmanović, D. Bolzoni, and P. H. Hartel, “A log mining approach for process monitoring in SCADA,” *Int. J. Inf. Secur.*, vol. 11, pp. 231–251, 2012.
[91] N. Goldenberg and A. Wool, “Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems,” *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 2, pp. 63–75, 2013.
[92] J. L. Rrushi, “SCADA protocol vulnerabilities,” in *Critical Infrastructure Protection*, Heidelberg: Springer-Verlag Berlin, 2012, pp. 150–176.
[93] J. Rrushi and R. Campbell, “Detecting cyber attacks on nuclear power plants,” *Crit. Infrastruct. Prot. II*, vol. 290, pp. 41–54, 2009.
[94] J. Edmonds, M. Papa, and S. Shenoi, “Security analysis of multilayer SCADA protocols: A Modbus TCP case study,” in *IFIP International Federation for Information Processing*, vol. 253, E. Goetz and S. Shenoi, Eds. Springer, IFIP Publications, 2007, pp. 205–221.
[95] J. Hieb, J. Graham, and J. Guan, “An ontology for identifying cyber intrusion induced faults in process control systems,” in *IFIP Advances in Information and Communication Technology*, vol. 311, C. Palmer and S. Shenoi, Eds. Springer, IFIP Publications, 2009, pp. 125–138.
[96] B. Zhu, “SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy,” in *WSCS 2010*, 2010, pp. 1–16.
[97] N. Goldenberg and A. Wool, “Accurate modeling of Modbus / TCP for intrusion detection in SCADA systems,” vol. 6, pp. 63–75, 2013.
[98] J. Beechey, “Application Whitelisting: Panacea or Propaganda?,” 2010.
[99] A. Nourian and S. Madnick, “A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet,” *Syst. J.*, no. September, pp. 1–12, 2014.
[100] Q. Chen and S. Abdelwahed, “A Model-based Approach to Self-Protection in SCADA Systems,” in *9th International Workshop on Feedback Computing (Feedback Computing 14)*, 2014, pp. 1–7.
[101] U. Tupakula and V. Varadharajan, “Techniques for detecting attacks on critical infrastructure,” in *Computing, Networking and …*, 2014, pp. 48–52.
[102] R. Mitchell and I. R. Chen, “A hierarchical performance model for intrusion detection in cyber-physical systems,” in *2011 IEEE Wireless Communications and Networking Conference, WCNC 2011*, 2011, pp. 2095–2100.
[103] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Basar, “Resilient control of cyber-physical systems against Denial-of-Service attacks,” in *2013 6th International Symposium on Resilient Control Systems (ISRCS)*, 2013, pp. 54–59.
[104] S. Pan, T. H. Morris, U. Adhikari, and V. Madani, “Causal event graphs cyber-physical system intrusion detection system,” in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 2013, pp. 1–4.
[105] U. Adhikari, T. H. Morris, and S. Pan, “A Causal Event Graph for Cyber-Power System Events Using

Synchrophasor," in *PES General Meeting | Conference & Exposition, 2014 IEEE*, 2014, pp. 1–5.
[106] F. Dorfler, F. Pasqualetti, and F. Bullo, "Distributed detection of cyber-physical attacks in power networks: A waveform relaxation approach," in *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2011, pp. 1486–1491.
[107] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework," in *Advances in Computer, Information, and Systems Sciences, and Engineering*, K. Elleithy, T. Sobh, A. Mahmood, M. Iskander, and M. Karim, Eds. Springer Netherlands, 2006, pp. 227–234.
[108] I. N. Fovino, A. Carcano, M. Masera, and A. Trom-Betta, *Design and implementation of a secure Modbus protocol*, vol. 311. Springer, IFIP Publications, 2009.
[109] C. Bellettini and J. Rrushi, "Combating memory corruption attacks on scada devices," in *IFIP International Federation for Information Processing*, vol. 290, M. Papa and S. Shenoi, Eds. Springer, IFIP Publications, 2008, pp. 141–156.
[110] J. Åkerberg and M. Björkman, "Exploring security in PROFINET IO," in *Proceedings - International Computer Software and Applications Conference*, 2009, vol. 1, pp. 406–412.
[111] J. Åkerberg and M. Björkman, "Exploring network security in PROFIsafe," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5775 LNCS, pp. 67–80.
[112] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proceedings of the IEEE Conference on Decision and Control*, 2011, pp. 2195–2201.
[113] A. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.
[114] R. Axelrod and R. Iliev, "Timing of cyber conflict.," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 111, no. 4, pp. 1298–303, 2014.
[115] J. Y. Keller and D. Sauter, "Monitoring of stealthy attack in networked control systems," in *Conference on Control and Fault-Tolerant Systems, SysTol*, 2013, vol. 0, pp. 462–467.
[116] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012.
[117] S. Amin, S. Amin, a. Cardenas, a. Cardenas, S. Sastry, and S. Sastry, "Safe and Secure Networked Control Systems under Denial of Service Attacks," *Hybrid Syst. Comput. Control*, no. 1, pp. 31–45, 2009.
[118] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Modeling security in cyber-physical systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 5, pp. 118–126, 2012.
[119] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, 2013.
[120] M. E. Kuhl, J. Kistner, K. Costantini, and M. Sudit, "Cyber Attack Modelling And Simulation For Network Security Analysis," in *Proceedings of the 2007 Winter Simulation Conference*, 2007, pp. 1180–1188.
[121] P. J. Hawrylak, M. Haney, M. Papa, and J. Hale, "Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid," in *Proceedings - 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012*, 2012, pp. 161–164.
[122] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli, and J. Wiley, "A testbed for secure and robust SCADA systems," *ACM SIGBED Rev.*, vol. 5, pp. 1–4, 2008.
[123] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Taxonomy for Description of Cross-domain Attacks on CPS," in *Proceedings of the {2Nd} {ACM} International Conference on High Confidence Networked Systems*, 2013, pp. 135–142.
[124] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS Attack Policy Against Remote State Estimation," in *52nd IEEE Conference on Decision and Control*, 2013, pp. 5444–5449.
[125] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attack on Cyber-Physical Systems: A game-theoretic approach," in *2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, 2013, pp. 252–257.
[126] C. Kwon, W. Liu, and I. Hwang, "Security analysis for Cyber-Physical Systems against stealthy deception attacks," in *2013 American Control Conference*, 2013, pp. 3344–3349.
[127] R. Saltzman and A. Sharabani, "Active man in the middle attacks : A Security Advisory," 2009.
[128] K. Chalkias, F. Baldimtsi, and G. Stephanides, "Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols," *Commun. Comput. Inf. Sci.*, vol. 23, pp. 227–238, 2008.
[129] T. T. Tran, O. S. Shin, and J. H. Lee, "Detection of replay attacks in smart grid systems," in *2013*

International Conference on Computing, Management and Telecommunications, ComManTel 2013, 2013, pp. 298–302.
[130] J. Kao and R. Marculescu, "Minimizing eavesdropping risk by transmission power control in multihop wireless networks," *IEEE Trans. Comput.*, vol. 56, no. 8, pp. 1009–1023, 2007.
[131] ICSJWG, "Protecting Critical Infrastructures from Emerging Cyber Threats Cyber Security by Design," S2013, 2013.
[132] C. W. Ten, C. C. Liu, and G. Manimaran, "Rent from DeepDyve »Vulnerability assessment of cybersecurity for SCADA systems," *Power Syst. IEEE …*, vol. 23, no. 4, pp. 1836–1838, 2008.
[133] P. Paganini, "Why humans could be the weakest link in cyber security chain?," *Security Affairs Website*, 2012. [Online]. Available: http://securityaffairs.co/wordpress/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html. [Accessed: 02-Oct-2015].
[134] H. Robert, "Humans 'often the weakest link' when it comes to cyber security," *NCC Group Website: New Room*, 2015. [Online]. Available: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/news/2015/july/humans-often-the-weakest-link-when-it-comes-to-cyber-security/. [Accessed: 10-Sep-2015].
[135] IRM, "Amateyrs attack technology. Professional hackers target people," *Website Article*, 2015. [Online]. Available: https://www.irmplc.com/issues/human-behaviour/. [Accessed: 15-Jun-2015].
[136] L. Navarro, "Train employees - your best defense - for security awareness," *SC Magazine Online*, 2007.
[137] M. Shalyt, "How Vulnerable are Our Industrial Control Systems? What We Learned From ICS Attacks of 2016," *Blog Post*, 2017. [Online]. Available: https://www.icscybersecurityconference.com/ust-vulnerable-industrial-control-systems-learned-ics-attacks-2016/. [Accessed: 25-Aug-2018].
[138] K. Townsend, "Ransomware Attack Disrupts San Francisco Rail System," *Security Week (Internet and Enterprise Security News, Insights & Analysis) - Online*, 28-Nov-2016.
[139] R. Nigam, "Threat Research: SCADA Security Report," *Fortinet Security Blog*, 2016. [Online]. Available: https://www.fortinet.com/blog/threat-research/scada-security-report-2016.html. [Accessed: 21-Aug-2018].
[140] T. Ball, "Top 5 Critical Infrastructure Cyber Attacks," *Computer Business Review (CBR): Online*, Jul-2017.
[141] L. H. Newman, "The Biggest Cybersecurity disasters of 2017 so far," *WIRED News Updates Website*, 2017. .
[142] D. Bolzoni, "Crashoverride: Protect your ICS network against the newest malware," *Security Matter Blog Website*, 2017. .
[143] D. Bolzoni, "ICS Malware conceived to disrupt operations found in the Middle East," *Security Matter Blog Website*, 2017. [Online]. Available: https://www.secmatters.com/blog/ics-malware-conceived-to-disrupt-operations. [Accessed: 21-Aug-2018].
[144] E. Kovacs, "Bad Rabbit Linked to NotPetya, but Not as Widespread," *Security Week (Internet and Enterprise Security News, Insights & Analysis) - Online*, 25-Oct-2017.
[145] UK-NCSC, "Advisory: Phishing campaign," *Security Alerts and Advisory Report*, 2018. [Online]. Available: https://www.ncsc.gov.uk/alerts/phishing-campaign. [Accessed: 22-Aug-2018].

Appendix Table A: ICS Cyber Security Incidents between 2015-2018.

YEAR	COUNTRY	META-DESCRIPTION
2016	UAE, Middle East	Spear-phishing email with attachment containing hawk eye malware which collect victim system's keystrokes, clipboard data and other information [137].
2016	Ukraine	Used Microsoft Excel documents with malicious macros via spam mail to compromise employee workstation with BlackEnergy malware on the Western Ukrainian power company Prykarpattyyaoblenergo. This enabled interference and the cut off of power to certain regions of the country [137].
2016	USA	Iranian Hacker gained unauthorised access to Bowman Avenue Dam control system in New York and gained critical system information [137]
2016	USA	Hackers breached Kemuri Water Company treatment plan through an outdated server and took control of several PLCs that controlled the flow of toxic chemical used for water treatment. Also it is believed that over 2.5 miilion customer payment information were stolen [137]
2016	USA	Ransomeware attack on San Francisco Municipal Transport Authority Train network, and disrupted internal computer system services including emailing [138].
2016	USA	Compromise of computer belonging to Calpine Contractor. Calpine is an electricity generation company. Company information including, network engineering schematics of 71 power stations across USA, network usernames and passwords stolen [139].
2016	USA	Spear-phishing attack used to compromise Wolf Creek Nuclear Power Plant and others [140].
2017	Global	WannaCry Ransomware infected thousand of public utility systems including National Health Service (NHS) hospital and facilities and disrupted normal operations [141].
2017	Global, Ukraine	Petya, NotPetya, Nyetya and Goldeneye ransomware infected several public utility systems including pharmaceuticals, shipping, and oil and gas, air and public transport, and power [141].
2017	Ukraine	CrashOverride (a.k.a. Industroyer) malware infected Ukrainian Power ICS network causing black outs [142].
2017	Middle East	Triton Malware infected industrial critical infrastructure facilities to take over control of safety instrumented systems [143].
2017	Russian & Ukraine	Bad Rabbit ransomware infected systems for media organisations in Russia, Transport (airport and subway) control system in Ukraine taking over systems and disrupting normal operations [144].
2018	UK	Phishing campaigns targeting several sectors running ICS such as transport, engineering and defence [145].