Current Applied Science and Technology Vol. 21 No. 1 (January-March 2021)

Review article

Digital Industrial Control Systems: Vulnerabilities and Security Technologies

Ibrahim Adepoju Adeyanju[1]*, Erhovwosere Donald Emake[1], Olatayo Moses Olaniyan[1], Elijah Olusayo Omidiora[2], Temitope Adefarati[3], Godwin Obruozie Uzedhe[4] and Nnamdi Stephen Okomba[1]

[1]Department of Computer Engineering, Federal University, Oye-Ekiti, Nigeria
[2]Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[3]Department of Electrical and Electronics Engineering, Federal University, Oye-Ekiti, Nigeria
[4]Department of Electrical and Electronics Engineering, Federal University of Petroleum Resources, Effurun, Nigeria

Received: 6 February 2020, Revised: 17 August 2020, Accepted: 28 August 2020

Abstract

Digital Industrial Control Systems (ICS) are complex electromechanical systems composed of components such as sensors, actuators, programmable logic controllers and communication devices interconnected to perform monitoring and control tasks in different industries. ICS have many and varied applications in critical infrastructures across the globe. However, security is an important factor for any ICS operation. In recent times, there have been a myriad of security threats and attacks by malicious elements on ICS, which has become a concern to organizations and researchers. The development of internet and communication systems has also exacerbated such security concerns. Activities of these malicious elements on ICS can result in serious disasters in industrial environments, human casualties and financial loss. Every ICS network element should be protected to avoid threats, attacks and maintain safe reliable infrastructure. Research efforts have been dedicated to improve ICS security for several decades and are still ongoing. This paper reviews ICS threats, vulnerabilities, cyber-physical attacks and security technologies over the last two decades (2000-2019).

Keywords: Industrial Control Systems; security; ICS; vulnerabilities; threats; cyber-attack; security technologies
DOI……

*Corresponding author: Tel.: +234 813 287 6689
E-mail: ibrahim.adeyanju@fuoye.edu.ng

1. Introduction

Digital Industrial Control Systems (ICS) are composed of various Information and Communication Technology (ICT) network components and associated devices that interact within a process loop to control physical entities [1]. These electro-mechanical complex systems respond to real-time data acquisition, system monitoring and automatic control and management of industrial processes [2]. Today, many nations and organizations' critical infrastructures rely on and are driven by ICS controllers to render control functions [3]. Currently, modern society controlled ICS processes include petroleum and gas refining [4], pipelines and distribution [5], electrical energy generation, transmission and distribution [6], water treatment and distribution [7, 8], chemical processing, pharmaceutical, food and beverage production, railway transportation and air traffic control [9]. ICS integrate computing and communication capabilities with monitoring and control of entities in the physical world [10].

There is a growing concern with respect to the abuse of technology devices associated with ICT and ICS environments including system networks and internet connectivity [11-13]. Implementation practices of ICS systems have introduced a wide range of security vulnerabilities [14]. Presently there is a very high rate of vulnerability and cyber-attacks globally on ICS; some of these threats and attacking agents includes terrorist network groups, dissatisfied employees, hostile governments and other malicious intruders [15]. Cyber- attack consequences are very devastating with effects ranging from disruption or damage of critical infrastructural operations [16, 3] to significant effect on public health, safety and destruction of lives and properties [15-18]. An in-depth understanding of the vulnerabilities, threats and attacks is crucial to the defense mechanisms and security methodologies of any ICS environment.

Security threats to ICS are becoming the biggest challenge for industrial system operations. Hence, it's vital to understand the current trend in the design of ICS, their threats, associated vulnerabilities and state-of-the-art security technologies that can serve as protection mechanisms. For the remainder of this paper, Section 2 gives an overview of Digital ICS, types and architectures while Sections 3 and 4 discusses the threats and vulnerabilities, respectively. The trend of Cyber-physical attacks on ICS is provided in Section 5 followed by a review of available security technologies and their limitations in Section 6. Section 7 maps digital ICS vulnerabilities and threats to appropriate security technologies. Section 8 concludes this review paper with a summary and projection towards improved and better secured digital ICS.

2. Overview of Digital Industrial Control Systems

Control Systems have been used in industries for real time control and monitoring of infrastructures. Critical infrastructures monitored and controlled by ICS are based on several types of field devices with information transmitted from remote station to master station. Supervisory and automated commands such as instruction to collect data from sensor connected with remote station can be initiated through the ICS communication field devices. Alarm status, breakers opening and closing status information and time synchronization check are enabled to effectively transmit data from control station or master station to field devices. ICS has a broad-based application in industrial environments ranging from production, supervision and corporate network.

Sensors, actuators, PLCs process units and communication devices are key components that are usually networked together in an ICS. A typical ICS environment is segmented into field device network or production network, supervisory and corporate network. An ICS could be exposed to vulnerabilities and cyber-physical attacks. This is especially true when the field device at the production network is driven by PLC devices connected to sensors and actuators. Usually, the

control system is equipped with wireless and wired communication capability designed with communication protocol for effective interaction among other ICS components.

2.1 Basic digital industrial control systems (ICS)

In an ICS operating environment, PLCs with different capabilities collaborate to attain various expected goals. The following are the basic digital ICS commonly used in manufacturing, oil and gas industry and other industrial environments [19]. They include:

Supervisory Control and Data Acquisition (SCADA): SCADA is usually deployed to control and manage long distanced assets accustomed with centralized knowledge acquisition and supervisory management. This means that operations are often monitored and controlled from another location at a long distance, typically with wireless facilities connected to facilitate operations [20-22]. SCADA reduces stress on staff from travelling to numerous operational sites when effectively deployed [23].

Distribution Control System (DCS): DCS is a control and monitoring mechanism used mostly in industries such as manufacturing, power generation, chemical producing, oil refineries, waste water treatment, etc. It encompasses a centralized design structure for supervision of the whole control loop. DCS is largely utilized in factories or on production sites; process parameters of the production plants are monitored and controlled with supervisory and regulatory control frame works within the working environment [24]. With several PLCs linked together as a distributed system, numerous tasks are effectively managed and performed. DCS is often utilized. However, actual implementation of ICS in industrial surroundings might typically be a hybrid of DCS and SCADA. Figure 1 clearly shows the basic forms of ICS and their functions.

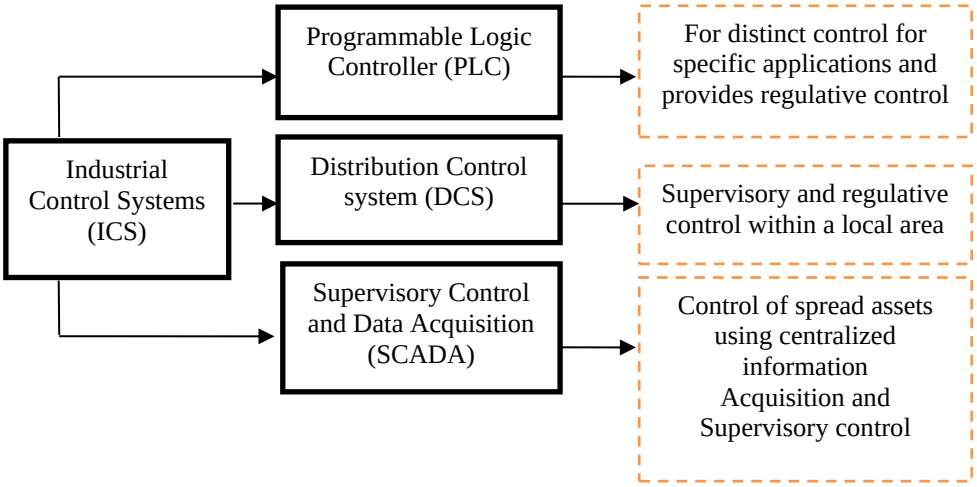

Figure 1. Basic forms of Digital Industrial Control Systems

Programmable Logic Controller (PLC): This is a skid mounted mechanism used for distinct control operations or specified applications, providing restrictive control [25, 26]. PLC is a hardware component domiciled in each DCS and SCADA system. The mounted device is equipped with capability of managing activities inside and delivers feedback signals that control devices like sensors and actuators.

2.2 Digital industrial control systems architecture

Each Digital Industrial Control System has a process loop system of both electronic and mechanical components [9] to control the physical operations of machines. Figure 2 shows the basic operation of an industrial control system. An operator issues set-points commands from the Human-Machine Interface (HMI) to machines, either domestically in-plant or via terminal control devices, typically named as field devices. The system then transmits detector information back to the controller making certain observance and control of the technical facilities to run mechanically and hitch-free. The functions of various ICS components are briefly highlighted.

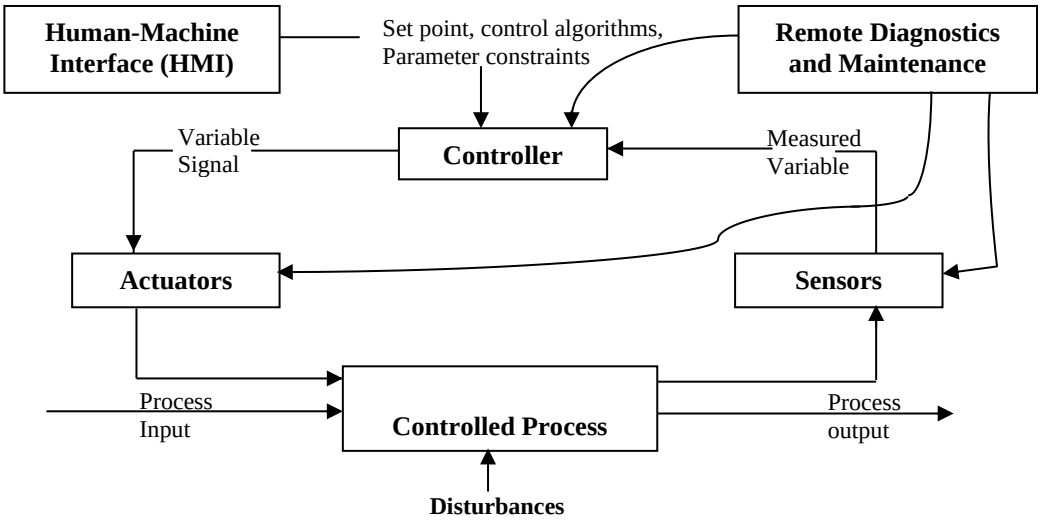

Figure 2. ICS Operation [9]

Control Loop: Various electronic/mechanical parts like sensors for measurement, controller hardware like PLCs, actuators like control valves, breakers, switches, motors, and communication of variables form the group as the ICS control loop, as showed in Figure 2. Interpreted signals from these interconnected parts are variables that are measured by sensors with the help of the controller.

Controller: The role of the controller housed by the PLC is to interpret the signals and generate the right processed variable output. The controller component accesses the issued set point commands from the HMI, then transmits signal to the actuators, but the complete method changes with any slight disturbances which might lead to new detector signals that have been known to vary the state of the method in restraint.

Remote Diagnostics and Maintenance Utilities: These maintenance utilities are extremely important in ICS operation, and are designed to stop system failure when enabled. They additionally have the potential to spot and help systems to recover from varied failure modes. Varied technologies and applications are incorporated in them for smooth functionality.

Human Machine Interface (HMI): HMI is the graphic interface unit that is capable of dealing with all human-machine interactions. The graphic interface is formed of hardware and software systems that enable operators' inputs to be translated as signals for machines that in turn give the specified result to the user. The HMI is employed for proper observation, configuration of

desired set-points and adjusting control formulas that likewise establish parameters within the controllers of an ICS.

2.3 Digital industrial control systems characterization

For better understanding of ICS operation and security approach, three basic characteristics associated with ICS were proposed: cyber, cyber-physical and physical [1, 27, 28].

Cyber characteristics: The feature of ICS which considers computational data, communications, and interactions that don't have any link with the physical world, i.e. physical infrastructure. However, due to communication and interaction between corporation's networks both within and outside ICS environment, these computational devices (controller) and other communication devices are now prone to cyber threats, vulnerabilities and threat attacks.

Physical characteristics: ICS with physical characteristics include any physical components present in the ICS architecture, e.g., sensors, actuators, etc. that their properties may be exposed to security concerns.

Cyber-physical characteristics: ICS with interactive devices and control data are open to the physical world. Therefore, there is the existence of digital interference in the entire ICS environment. Here, the cyber aspect and physical world has a communication link. Today this category of ICS is common as most organizations and their operations are connected to/through the internet. Modern ICS integrate both information technology (IT) and industrial components working together to achieve industrial set goals. These components are varied into layers of functionalities and operations [27, 29].

3. Threats to Digital Industrial Control Systems

Threats confronting ICS are numerous with several sources including malicious intruders, terrorist teams, hostile governments, dissatisfied staff, industrial spies and natural sources such as system complexities, instrumentation failures and natural disasters [30, 10]. This paper outlines four possible classifications of threats facing industrial control systems and briefly describes their activities in the ICS environment.

Adversarial threats: This threat poses malicious intentions from individuals such as script kiddie, hackers, industrial spies, cyber warriors, terrorist groups, or from organizations including competitors, suppliers, partner firms and hostile governments of nations/states [10]. The activities of this adversarial threat targets cyber resources, exploiting available ICT capabilities. The available data and resources become their motivational drive. They initiate and sustain distributed attacks on digital ICS whose networked components are exposed to the internet. The role of malicious internal/insider threat actors, e.g. disgruntled employees or dissatisfied staff, are clear examples of this threat category.

Structural threats: This embodies information technology (IT) related devices such as storage device, processing and communication equipment, sensors, controllers and power supply software [10]. Most examples of structural threats occur as a result of ageing or outdated software packages, breakdown or conditions that exceed expected operational parameters. Their effects are very disruptive and devastating to personnel and ICS operation.

Accidental threats: Equipment handlings by employees are the major cause of this class of threat. It also embodies inaccurate steps taken by instrumentation handler, operators or individual within the course of executing daily tasks.

Environmental threats: This includes natural or artificial disaster (e.g. fire, flood/tsunami, windstorm/tornado, hurricane, earthquake, bombing, overrun), uncommon natural incidence (e.g.,

sunspots), infrastructure failure, telecommunications or electrical power outage [31, 10]. This threat also has a large-scale effect on industrial control systems.

4. Existing Vulnerabilities in Digital Industrial Control Systems

Classification of Digital ICS vulnerabilities can assist in taking proactive steps in implementing applicable security approaches. It has been discovered recently that almost all types of attacks on ICS can be orchestrated and that a substantial range of those attacks are because of the vulnerabilities of industrial applications [32, 33]. The exposure of a system to any potential attack is understood as system vulnerability [34]. One major event that played out on ICS vulnerabilities and security was the Stuxnet Microsoft Windows PC worm discovered in July 2010 that specifically targeted the industrial software system of an Iranian nuclear facility. Stuxnet exploited several vulnerabilities within the execution space and also within the ICS protocol implementation [35]. Hidden in the industrial facilities, the virus was made to spread through U-disk and other system equipment in the local area network, [36, 37] controlling the operation of the centrifuge system using the vulnerabilities of the operating system. ICS vulnerabilities are, therefore, categorized into six groups: Policy and Procedure, Architecture and Design, Configuration and Maintenance, Physical, Software Development, and Communication and Network Configuration Vulnerabilities [10].

Policy and Procedure Vulnerabilities: This vulnerability is a result of poor ICS security audit policies, lack of ICS specific configuration change management, inadequate formal training and awareness program on ICS security measures and lack of administrative mechanisms for security enforcement. Other reasons for this vulnerability include inadequate security on architecture and design, lack of specific continuity of operations or disaster recovery plans, and inadequate programs plans and procedures for detection and response to security breach. Solutions to this type of vulnerability include routine training of control engineers on security of ICS, design of specific security procedures, and guidelines on equipment implementation with regular updates. Prioritized incident detection and response to minimize loss and destruction should be the main features of the designed ICS security procedures.

Architecture and Design Vulnerabilities: This vulnerability is due to factors such as inadequate data collection of event history, insufficient integrated security features in ICS architecture, and undefined security perimeters. Solutions include retention of accurate, proper and sufficient data to determine future security breaches, routine security monitoring to identify security controls issues, and clearly defined security perimeters that are vital to ensure proper security control configuration to avoid unauthorized access to systems and data.

Configuration and Maintenance Vulnerabilities: These are a function of improper configuration management, update patches in operating system without exhaustive testing, inadequate testing of security changes, unsecured passwords generation, Denial of Service (DoS), and insufficient authentication/access control for the configuration and other software. Other factors include improper identification of security breaches, ineffective real-time monitoring of logs and endpoint sensors, and insufficient testing of installed anti-virus software in the ICS environment. Counter measures to this vulnerability include effective use of software to prevent DoS attacks, crucial software testing before deployment and proper keeping of accurate logs to detect security breaches.

Physical Vulnerabilities: These include lack of backup power, voltage spikes due to radio frequency, electromagnetic pulse (EMP) or static discharge, loss of environmental control, unsecured physical ports and unauthorized personnel having physical access to ICS equipment. Possible solutions are proper shielding, grounding and surge suppression of electrical equipment, disabling all universal serial bus (USB) and PS/2 ports, and restrictions on personnel who have

physical access to the ICS environment. Safety requirements, such as emergency shutdowns or restarts to avoid disaster should also be put in place.

Software Development Vulnerabilities: Causes of this type of vulnerability include inadequate authentication, privileges, and access control in software, installed security capabilities not enabled by default and improper data validation. Solutions are prevention of unauthorized access with proper configuration and the enabling of installed ICS security capabilities.

Communication and Network Configuration Vulnerabilities: These are caused by non-existent or improperly configured firewalls, insecure industry-wide ICS protocols, authentication issues traceable to both wireless clients and access points, inadequate data protection between wireless clients and access points. The proper configuration of firewalls between networks, such as corporate networks control, is required to prevent unnecessary data flow and attacks from malware. A solution to this vulnerability is to place priority on data flow controls and restriction of information among systems based on data characteristic. Other solutions include the keeping of accurate and proper logs, enforcement of standard ICS protocol authentication at all levels.

5. Cyber-Physical Attacks and Digital Industrial Control Systems

Digital ICS operations are safety-critical, since they are employed in wide application domains. Their disruption/failure, whether accidental or intentional, will have harmful results on our society at large, damaging infrastructures, property and even persons. The cyber-attacks on the Ukrainian electrical grid [38] and the Mirai attack [39] are a handful of legendary events that followed the Aurora experiment, where an engine was attacked and destroyed solely by cyber means [40]. The Aurora experiment was the first documented cyber-attack on ICS that caused serious damage to the Iranian nuclear program.

5.1 Impact of cyber-attacks on industrial control system operations

The impact of cyber-attacks on ICS environment depends on the target's nature of operation or the motivation of cyber criminals following the attack. Impact can be internal or external. Common techniques of ICS cyber-attacks and related potential impact include the following [41]

- *Changes observed by altering system operations application configurations*: Once systems set-point data or vital parameters are altered, unwanted or unpredictable outcomes result. Such change could be done to mask malware behavior or any malicious activity. These could also conjointly have an effect on the output of a threat actor's target.
- *Change in PLC, RTUs and other controllers:* Observed changes in controllers and other associated devices can equally lead to damage of equipment or facilities. These can further cause control process malfunction and disable control over a process.
- *Misinformation in line with operations*: False or misleading operational commands could lead to implementation of unwanted or reserve actions owing to wrong knowledge. Such an occurrence might modify the programmable logics. This can jointly facilitate concealment of malicious activity, which is the incident itself or the injected code.
- *Alteration of safety controls procedures*: Forestalling the proper operation of safety measures can endanger the lives of workers, and external clients might be put a risk.

5.2 Possible consequences of ICS cyber-attacks

The securing of systems is vital and compelling as business reliance on interconnectivity increases on a daily basis. However, Denial of Service (DoS) attacks and malware (e.g., worms, viruses) are becoming extremely common and have a direct impact on ICS. Cyber-attacks usually have physical and eventful effect. Consequential impacts of ICS attacks can be classified as follows [10]:

Physical Impacts: This type of impact underscores a set of direct consequences of ICS failure. Effects of this impact include personal injury and loss of life damage/loss of property associated with ICS environment. Physical impact is categorized as first order impact in terms of degree of assessment.

Economic Impacts: ICS incidents occur with a strong resultant physical impact. Physical impacts may result in repercussions to system operations that in turn lead to a bigger economic sabotage on the production facilities, organization, or other equipment that are dependent on the ICS. Unavailability of necessary infrastructure (e.g., electric power generation and distribution, transportation) can have a high economic impact. These effects may negatively impact the native, regional, national or presumptively international economy. Economic impact is categorized as second order impact in terms of degree of assessment.

Social Impacts: The consequences of this impact result from the loss of public confidence in a company, with failed ICS due to cyber-attacks. Social impact consequences can be very unpleasant and dreadful. Social impact is categorized as second order impact in terms of degree of assessment.

5.3 ICS cyber-physical attacks

The control loop of a typical ICS constitutes an industrial process application view which can be implemented following a hierarchy of industrial computing systems that makes it vulnerable to threat attacking agents. The controller, which is usually known as the PLC, is a system that implements two logical processes: (a) it controls autonomously the connected device(s) at the lower level of the hierarchy, and takes in input device information and controlling actuators, and (b) it executes a part of a distributed application that controls the complete plant underneath the direction of the SCADA system, and acts with the SCADA system and presumably with different PLCs [42, 28].

ICS can therefore be said to be exposed to computational attacks and data attacks in a cloud-based environment. Although clouds are much more vulnerable to associated threats just as is the internets, both are important factors in ICS operation. Therefore, to successfully secure digital ICS, sophisticated techniques are needed to equally secure clouds. Usually, a cloud is built with the help of the internet with both having security concerns on ICS operations. Although access to data in a cloud-based environment is made possible using virtual machines via the internet, both client and provider reside at their separate geographical areas [43, 44]. Cloud computing environments ensure easy access to ICS operational data at any time and at any location.

Digital ICS cloud-based environment requires standard protocols to effectively provide efficient security for operational parameters/other process control data during transmission. Two basic types of attacks on ICS cloud-based environments are internal/insider and external attacks [45].

Insider/Internal Attacks: This attack type leverages on the open platform in clouds. They are very high-risk and harmful compared to external attacks. These attacks are caused by valid or legitimate users of clouds, who gain access to networks in the following manners: Packet Dropping, Device Isolation, Route Disruption, Modification Based Attacks, and Attacks Based on Fabrication [45]. Attackers can easily bypass the security mechanisms because of the various access links they

have to the system. They can as well gain access to the services of Cloud in a normal manner, therefore, proactive measures on internal attacks generated by the malicious insider devices call for huge attention [45-47].

External Attacks: External attack causes congestion by introducing and propagating fake routing information thereby preventing connecting devices from providing active services. External attacks within the cloud are almost like external attacks in a traditional computing environment. Attacks of this type can be effectively handled by preventive measures and employing techniques like firewall or authentication to detect attacks in ICS environment.

5.4 Cyber-attack classification

A detailed classification of cyber-attacks on digital industrial control systems (ICS) is diagrammatically presented for a better understanding of threat attacks associated with ICS. Figure 3, shows ICS attacks (internal/insider or external) further grouped into four attack classification; (i) reconnaissance (ii) response and measurement injection (iii) command injection, (iv) denial of service. Seventeen types of attacks under the above mentioned four classifications were further identified as current cyber-attack on ICS-MODBUS communication protocol [48, 49].

Reconnaissance: Intelligent attackers gather system network information, map the network architecture and determine the device characteristics like manufacturer model number, supported network protocols, system address and system memory map. Four intelligence operation attacks against MODBUS servers include; the address scan, the perform code scan, the device identification attack and also the points scan. The address scan consistently scans to find ICS servers configured to a network. The perform code scan identifies supported network operations which can be performed for an associate noted server. The device identification attack permits an associated attacker to be told a discovered device's trafficker name, product code, major and minor revision, et cetera. The points scan permits the offender to create a device memory map [49].

Response and Measurement Injection Attacks: This kind of attack occurs in ICS without adequate authentication tools to check that the real source of received data packets during polling is real. Polling is a method used for remote operations, where each transmitted query returns a response packet, containing sensor readings, between clients and the server. Such responses are saved as measurements to influence the feedback control loop. Intruders can inject the response packets and modify to give wrong sensor values. Without effective authentication to identify the packet source, the ICS can be injected with wrong sensor values which can adversely affect the ICS. Response injection attacks are classified into two categories; Naive Malicious Response Injection (NMRI) attacks and Complex Malicious Response Injection (CMRI) attacks.

Command injection: In the type of attack, incorrect commands (control/ configuration) are sent into a control system to cause sabotage. Because supervisory control actions are taken by human operators, intruders can try to mimic the operators to inject supervisory actions to exploit the control system. The activities of this category of attacks by hackers focus on remote terminals coded typically with C programming language using ladder logic and registers to implement their goals. Possible effects of command injections include unauthorized alteration of device configurations, interruption of ICS device communications, unauthorized adjustment of process set points and interruption process control. The malicious command injection attacks by hackers are grouped into three categories as shown in Figure 3; Malicious State Command Injection attacks, Malicious Parameter Command Injection attacks, and Malicious Function Code Injection attacks.

Denial of Service Attacks: Denial of Service (DOS) attacks against ICS attempt to stop some portion of the cyber physical system completely from functioning in other to effectively disable the entire system. DOS attacks would possibly target the cyber system or the physical system. DOS cyber system attacks target communication links, disabling programs running

on system endpoints that control the system, log data, and govern communications. DoS attacks on physical system vary from the manual opening or closing of valves and switches to destruction of components of the physical process that forestall operation [47-51]. The aim is to crash the PLC by sending a very large number of packets within a very small-time frame [52].

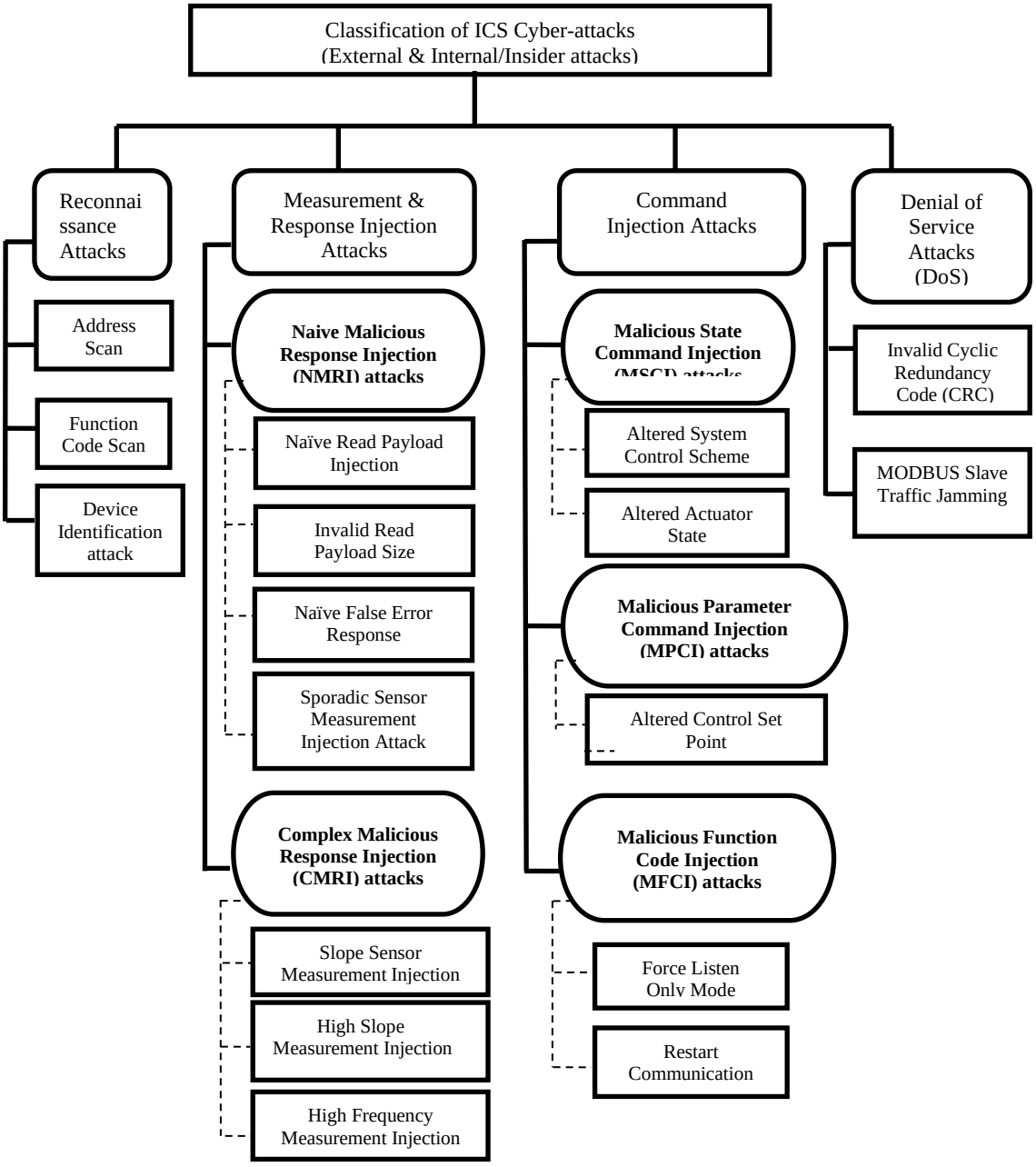

Figure 3. Types of attacks on ICS-MODBUS Communication protocol [49]

6. Security Technologies for Digital Industrial Control Systems

Digital ICS have wide application in critical infrastructure across the globe. Malicious attacks on ICS by threat agents can lead to serious consequences [47]. Therefore, a proactive security measure is an important factor to protect these critical infrastructures. In this section, current security technologies employed in Digital ICS environments to secure them from threat attacks are discussed. Generally, current ICS security technologies can be classified into two broad technologies [6] as shown in Figure 4.

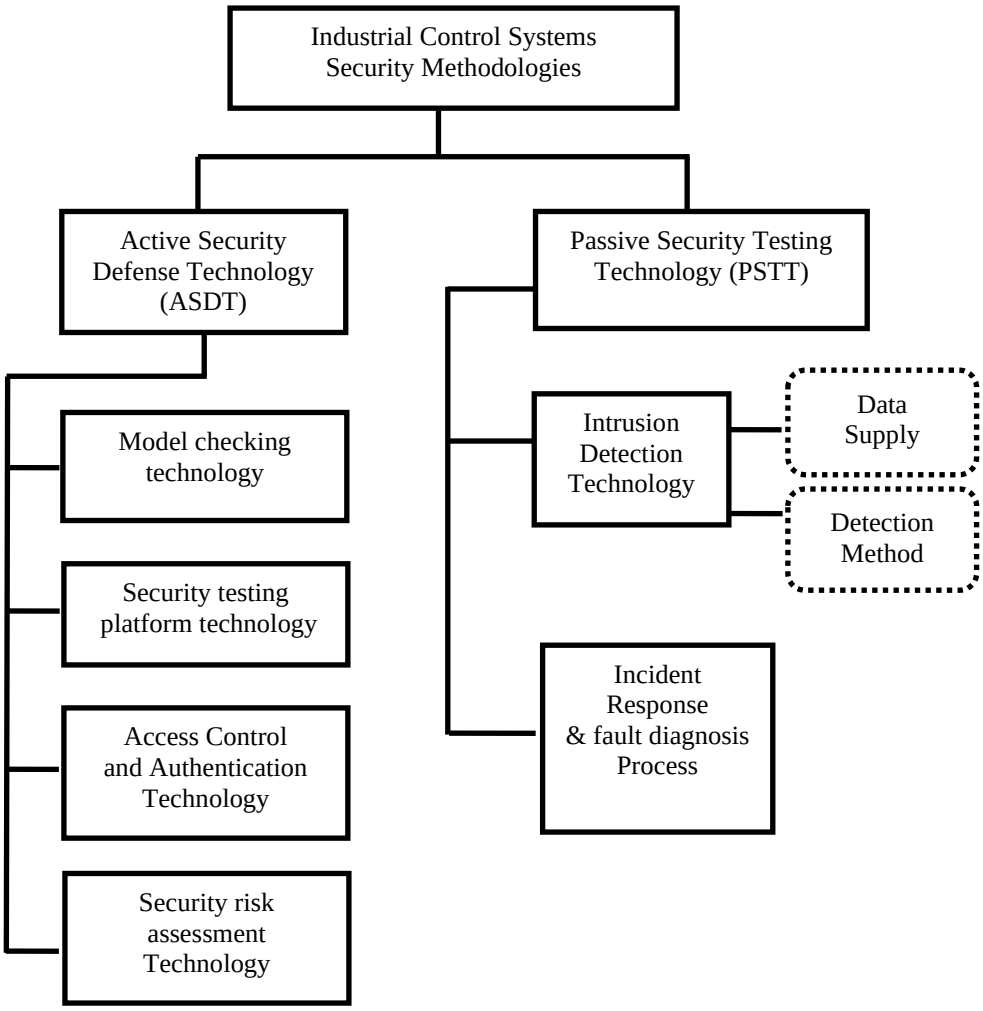

Figure 4. ICS security methodologies [6]

6.1 Active security defense technology

Four techniques are defined under this class of security technologies: They include:

Model checking: This focuses on applying information technology (IT) to ICS security [53]. Considering a recent incident of ICS attack, Stuxnet, a sophisticated cyber software worm that targets SCADA in critical infrastructure companies was found to have been uploaded on the PLC that control industrial automation processes [54]. Additionally, the internet worm allowed attackers to gain total control of critical operations of a process plant from remote locations [55]. In order to effectively handle ICS security flaws, a security mechanism, known as simple non-programmable hardware chips or STCB, to secure ICS/SCADA systems was developed [56].

The low complexity of STCB chips permits verification and facilitates the building block of complicated trusted functionalities of system controllers [57]. However, this security approach assumes that all functional processed data from sensors and actuators are seen to be impersonated by malicious attacks [6]. To enhance this, an associated approach was developed to facilitate a semi-automated security system verification of control systems by a completely unique application of model checking. This was made possible by a research group who enjoyed considerable success recorded with a technique that used historically automated software package verification. The designed model was completely different from model-checking applications, and it had the flexibility to uncover missing safety and security properties that ought to forestall catastrophes caused by malicious activities [56, 58].

Another security approach using checking model technology was demonstrated for High Integrity Communications (HIC). A subversion-resistant guard was built with the help of GEMSOS (GemSeal guards) based on the network ahead of every existing component like the controllers and edge clients. This security approach used seal packets that are sent between controllers and edge clients with a label for their source. The guards forward every labelled packet across the un-trusted network to a guard at the destination with solely crypto seal that binds a label to an identical destination label allowed but unlabeled or altered packets cannot enter the destination [57, 59].

Security testing platform: Recent discovery on proliferation of cyber-attacks on ICS shows that large numbers of security vulnerabilities exist in ICS [33]. However, the ever-increasing rate of attacks on ICS resulted in the development of security test-beds that became very crucial for the evaluation of the protection of ICS tools and products. One among such test-bed designed security models was for evaluating the security of industrial applications by providing completely different metrics for static testing, dynamic testing and network testing in industrial settings. Comparing the model with alternative detection platforms, this platform covered all components of ICS and provided metrics for evaluation [60]. Also proposed was another security solution that used cryptography applications to protect communication (SCADA/DNP3 protocol communication) from abnormal attacking scenarios. This was based on existing and current SCADA/DNP3 associated security issues within each test-bed that was implemented [61]. The demonstrated scheme effectively compensated for the shortage of performance of the firewall, and IPsec SSL/TLS in a digital ICS environment.

Authentication and Access Control: This technology establishes access management for ICS by checking to ascertain if user's credentials are on identical page to the credentials readily available on database of licensed users or in a data authentication server. Any process by which a system carries out verification and identification of a user who wishes to access the system is known as authentication. However, access control is typically based on the identity of the user who requests access to a resource. Authentication is essential to effectively secure control systems, and to execute this security strategy, user authentication is therefore implemented through credentials which at a minimum consist of a user ID and password. Distributed firewalls are deployed and been added as protective layer among internal subnet compared with traditional boundary firewall [62]. Firewalls

sit between a router and application server to provide access control. Router configurations add to the collective firewall capability by screening the data presented to the firewall.

Security risk assessment: Understanding security risk assessment process can be useful for security engineers, inspectors, insurance underwriters and general quality assurance/audit staff. Security risk assessment can be helpful for ICS operations and maintenance personnel who can offer some new perspective on the facilities' risk posture. The key aspect of this technology is that it simply identifies problems and their associated risks as a starting point in order to avoid waste of time and resources. This technology is very important for the mitigation of identified risks.

6.2 Passive security testing technology

Two main techniques are identified under this class of security technology: Intrusion Detection Technology and Incident Response and Fault Diagnosis Process [6].

Intrusion Detection Technology: Intrusion detection is a passive security defense strategy that observes and analyses the events taking place in an information system with the aim of discovering signs of security issues [63]. It consists of a device or software application that monitors systems network behavior, and IDT gathers and analyses system information for malicious activity or policy violations [64]. Any discovered malicious activity or violation is typically reported or collected centrally using a security information and event management system. IDT detects whether there is intending disruption in form of attack against digital ICS systems by continuously comparing with known intrusion model or making decision and analysis for the unknown intrusion model [6]. In IDT, new detection rules are created specifically for ICS systems, and communication protocol in networks are equally designed with the needed specification. These new rules in the designed model are mainly based on attack signatures, anomaly detections, probabilistic models, system specifications as well as the behavior of ICS components [65]. Iterative estimation of Hurst parameter for rapid detection, advanced samplings for classification of anomaly detection, and network intrusion detection with semantics-aware capability have been previously proposed [66-68]. Information theory has been described based on the concept of symbolic dynamics known as a data-driven technique [69]. Statistical technique for detection of network anomalies was proposed and became known as the signal processing approach [70]. Later, intrusion technique for ICS effective operation was proposed and immediately deployed [71, 72]. The intrusion detection system (IDS) uses different data sources available from the monitored ICS. This detection technology detects the presence of an intrusion and immediately sounds an alarm, prompting response to the threat agent wanting to disrupt ICS operation. IDS is classified and determined by the type of information source and the detection techniques used [73]. The effectiveness of IDS techniques and their application in Cyber physical systems is founded on a two design and classification approach namely the detection approach and the audit material approach [74].

Incident Response and fault diagnosis Process: A comprehensive incident response is a significant tool in ICS cyber security, taking cognizance of the various threat attacks facing enterprises. ICS threats are counted to be among the foremost critical aspect of a nation's infrastructure. Mis-configuration, human error, failure, and attackers target ICS and cause them to lose availability and integrity [6]. Emergency response and fault diagnosis ability helps further protection and safety for ICS. In this approach a defense strategy called "Defense in Depth", which describes the configuration of each defense layer, is shown in Figure 5. Before an exploitation of zero-day attack can affect the system, a multilayered defense with safety functions initiates and perform certain emergency actions. Moreover, even with minimal software installation and network connections, the system acts robustly against unknown cyber-attacks. To improve security concerns, ICS network security incident response and troubleshooting process was proposed [75]. The goal of the incident response set up is to permit the organization to manage the cost and injury related to

incidents and to enable a faster recovery of the cost systems [76]. Security incidents in ICS can be very harmful to systems and networks.

6.3 Depth defense strategy

Overall, complete digital ICS security cannot be achieved solely on a single security technology solution. Therefore, it becomes imperative to integrate a range of security technologies hierarchically to boost the defense capability of industrial systems.

The United States Department of Home Security [32] proposed a "defense in depth" strategy, as shown in Figure 5 [6]. The model is segmented into five layers. The first layer is the use of commercial firewalls. The deployment and use of firewall, intrusion detection, vulnerability scanning and other proactive security measures can be helpful in mitigating possible ICS attacks acting as an integral protection [32, 77].

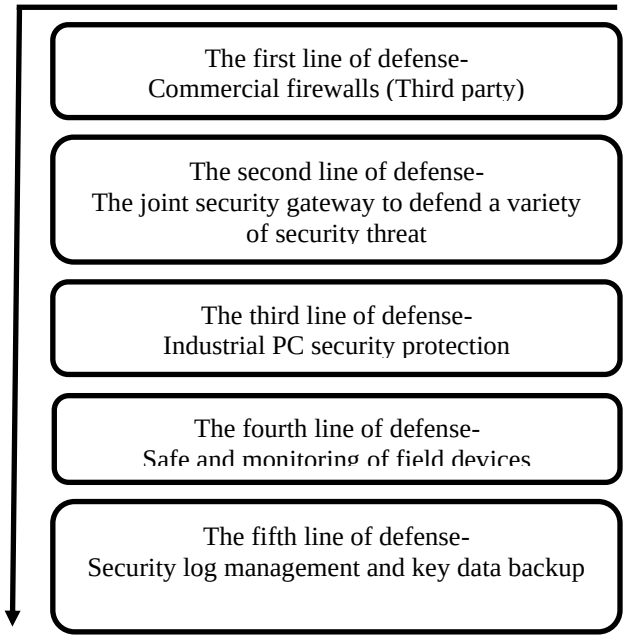

Figure 5. ICS security defense in depth model [32, 6]

Man-in-the-Middle attacks can be averted by securing field device communications networks by deploying and safe guarding the environment using field level firewalls designed for PLCs, IEDs, and SCADA RTUs [78]. The second layer is the joint security approach to defending from a variety of security threats. This is done by insulating the office network from external network using commercial firewalls, while attention is placed on security gateway which mainly insulates work area to control area. The third layer is the protection and security of industrial PCs from prevailing threat attacks and vulnerabilities. The fourth layer is the monitoring of field devices, while security log management and data backup is taken care of by the fifth layer.

7. Mapping Digital ICS Vulnerabilities to Security Technologies

This paper has presented a detailed and comprehensive analysis of current digital ICS threats attack, vulnerabilities, and available ICS security technologies designed to effectively handle prevailing ICS attacks. In this section, different categories of vulnerabilities are mapped to appropriate security technologies for a better analysis. Table 1 summarizes these mappings.

Categories of digital industrial control systems' vulnerabilities have distinct attacking methods which can be handled with different security technologies. Detailed control strategies are highlighted as part of the security technologies for each specific vulnerability; these control approaches are a vital aspect of ICS security. It is advisable that organizations should always prepare employees working in ICS environment with all necessary training for safe and secured operations.

Table 1. Vulnerabilities, attack method and corresponding security techniques in a digital ICS environment adapted from Stouffler *et al*. [10] and Fielder *et al*. [79]

S/N	Vulnerabilities category	Attack Method (Type)	Security Technology	Control description
1	Policy & Procedural Vulnerabilities	-Social Engineering (External)	Security Risk Assessment Technology	- Specific security procedures - Documented formal security training and awareness program for employees
2.	Physical Vulnerabilities	-Removable device driver malware (External)	Security Testing platform Technology	- Consistent and effective defensive posture, removable media check before use
3	Architecture and Design Vulnerabilities	-Malicious Remote Access (External)	Access control Authentication Technology	- Unauthorized access control
4	Architecture and Design Vulnerabilities	-Cross site scripting (External) -SQL command injection, removable device driver Malware, Buffer overflow, Man- in -Middle (Internal)	Model Checking Technology	- Network data validation & integrity check - Retention of accurate, proper & sufficient data to determine future security breach
5	Software Development Vulnerabilities	- Internet Malware, Removable device driver Malware (External) - LAN based Injection (Internal)	Model Checking Technology	- Anti-virus software
6	Communication and Network Configuration Vulnerabilities	- Internet Malware, Malicious Remote Access (External) - Authentication Bypass, Removable device driver malware, Buffer overflow, Man- in -Middle (Internal)	Intrusion Detection Technology	- Demilitarization and Firewalls
7	Configuration and Maintenance Vulnerabilities	- Malicious Remote Access (External) - Authentication Bypass & Misuse of Access Authority (Internal)	Incident Response & Diagnosis Technology	- Consistent and effective defense posture. - Standard & adequate anti-virus

8. Conclusions

An in-depth review on digital industrial control system architectures, threat attacks and vulnerabilities is presented in this paper. One major concern across the globe is the security of critical infrastructures that are basically driven by Digital Industrial Control Systems (ICS). Many such critical infrastructures are facing huge cyber-attacks with consequential impact on the economies of the affected nations. Cyber-attacks on ICS poses serious threats to lives and properties. Today, ICS are also exposed to new threat agents, due to internet-connectivity in most industrial environment and this situation calls for more proactive security solutions, especially with the cyber-physical aspects of ICS. Although significant progress has been recorded in the development of varied techniques for securing digital ICS, more security solutions are needed to combat the new wave of cyber-physical attacks on critical infrastructures across the globe. This paper reviewed modern security technologies that when carefully studied will be very useful for ICS security researchers, assets owners and organizations who seek to build more proactive security solutions that will help in tackling threat attacks and vulnerabilities associated with ICS.

References

[1] Coletta, A. and Armando, A., 2015. Security monitoring for industrial control systems. *Proceedings of the 1st Conference on Cybersecurity of Industrial Control Systems, CyberICS 2015, and the First Workshop on the Security of Cyber Physical Systems, WOS-CPS 2015*, Vienna, Austria, September 2015, LNCS 9588, 48-62.

[2] Hu, Y., Yang, A. Li, H., Sun, Y. and Sun, L, 2018. A survey of intrusion detection on industrial control systems. *International Journal of Distributed Sensor Networks*, 14(8), https://doi.org/10.1177/1550147718794615

[3] Obodoeze, F., Obiokafor, F.N. and Asogwa, T., 2018. SCADA for national critical infrastructures: Review of the security threats, vulnerabilities and countermeasures. *International Journal of Trend in Scientific Research and Development*, 2(2), 974-982.

[4] Weiss, J., 2010. *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum Press.

[5] Hentea, M., 2008. Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management*, 3, 73-86.

[6] Fan, X., Fan, K., Wang, Y. and Zhou, R., 2015. *Overview of Cyber-security of Industrial Control System*. [online] Available at: http://toc.proceedings.com/27630webtoc.pdf

[7] Cardenas, A.A., Amin, S. and Shankar, S., 2008. *Research Challenges for the Security of Control Systems*. [online] Available at: https://people.eecs.berkeley.edu/~sastry/pubs/Pdfs%20of%202008/CardenasResearch2008.pdf

[8] Uchenna, P., Ani, D., Hongmei, M.H. and Tiwari, A., 2016. Review of cybersecurity issues in industrial critical infrastructure; manufacturing inperspective. *Journal of Cyber Security Technology*,1(1), 32-74.

[9] Stouffer, K., Falco, J. and Scarfone, K., 2013. Guide to industrial control systems (ICS) security, *NIST Special Publication 800-82 Revision 1*, http://dx.doi.org/10.6028/NIST.SP.800-82r1

[10] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A., 2015. Guide to industrial control systems (ICS) security. *NIST Special Publication 800-82 Revision 2*, http://dx.doi.org/10.6028/NIST.SP.800-82r2

[11] Alcaraz, C. and Zeadally, S. 2013. Critical control system protection in the 21st century. *Computer* 46(10), 74-83.

[12] Miller, B. and Rowe, D., 2012. A survey of SCADA and critical infrastructure incidents. *Proceedings of the 1st Annual conference on Research in information technology*, October 2012, 51-56.
[13] Shaw, W.T., 2006. *Cybersecurity for SCADA Systems.* Tulsa: PennWell Corp.
[14] Sajid, A., Abbas, H. and Saleem, K., 2016. Cloud-assisted IoT-Based SCADA systems security. A review of the state of the art and future challenges. *IEEE Access*, 4, 1375-1384.
[15] Radvanovsky, A. and McDougall, R., 2009. *Critical Infrastructure: Homeland Security and Emergency Preparedness*. 2nd ed. Boca Raton: CRC Press.
[16] Hathaway, O.A., Crootof, R., Levitz, P. Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. 2012. The law of cyber-attack. *California Law Review*, 100(4), 817-885.
[17] Bernard, T., Hsu, T., Perlroth, N. and Lieber, R., 2017. *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.* [online] Available at: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.
[18] Bisson, D., 2017. *10 of the Most Significant Ransomware Attacks of 2017.* [online] Available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/10-significant-ransomware-attacks-2017/
[19] Lu, T., Guo, X., Li, Y., Peng, Y., Zhang, X., Xie, F. and Gao, Y., 2014. Cyberphysical security for industrial control systems based on wireless sensor networks. *International Journal of Distributed Sensor Networks*, 10(6), 1-17.
[20] Kim, T.H., 2010. Integration of wireless SCADA through the internet. *International Journal of Computers and Communications*, 4(4), 75-82.
[21] Kovaliuk, D.O., Huza, K.M. and Kovaliuk, O.O., 2018. Development of SCADA system based on web technologies. *International Journal of Information Engineering and Electronic Business*, 10(2), 25-32.
[22] ENISA, 2007. *A Strategic Approach to Protecting SCADA and Process Control.* [online] available at*:* http://documents.iss.net/whitepapers/SCADA.pdf, 2007
[23] Butts, J. and Shenoi, S., 2014. Critical infrastructure protection VIII. *Proceeding of the 8th IFIP WG 11.10 International Conference, ICCIP 2014*, Arlington, VA, USA, March 17-19, 2014, 65-78.
[24] Anand, S., Sarkar, S. and Rajendra, S., 2012. Application of distributed control system in automation of process industries. *International Journal of Emerging Technology and Advanced Engineering*,, 2(4), 377-383.
[25] Kiran, A.R., Sundeep, B., Vardhan, S.C. and Mathews, N., 2013. The principle of programmable logic controller and its role in automation. *International Journal of Engineering Trends and Technology*, 4(3), 500-502.
[26] Wang, C., Liu, M.X.A. and Zhang, J., 2017. The application of PLC control system in oil and gas pipeline transportation. *Proceeding of the 2nd International Conference on Mechanical Control and Automation (ICMCA)*, doi:10.12783/dtetr/icmca2017/12334
[27] Peng, Y., Wang, Y., Xiang, C., Liu, X., Wen, Z., Chen, D. and Zhang, C., 2015. Cyber-physical attack-oriented industrial control systems (ICS) modeling, analysis and experiment environment. *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 322-326, doi: 10.1109/IIH-MSP.2015.110
[28] National Institute of Standards and Technology, 2016. *Framework for Cyber-Physical Systems. Volume 1, Overview*. National Institute of Standards and Technology (NIST) Special Publication 1500-201, US Departemnt of Commerce, USA.
[29] Didier, P., Macias, F., Harstad, J., Antholine, R. and Johnston, S.A. 2011. *Converged Plantwide Ethernet (CPwE) Design Implementation Guide*. [online] Available at: https://belorg.by/wp-content/uploads/rockwell/td/enet-td001_-en-p.pdf

[30] Rao B.S., Chakravarthi, C.V. and Jawahar, A., 2017. Industrial Control Systems Security and Supervisory Control and Data Acquisition (SCADA). *International Journal for Modern Trends in Science and Technology*, 3(10), 109-118.

[31] Kang, D., Lee, J., Kim, S. and Park, P., 2009. Analysis on cyber threats to scada systems.. *2009 Transmission & Distribution Conference & Exposition: Asia and Pacific*, doi: 10.1109/TD-ASIA.2009.5357008.

[32] DHS, 2009. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, Control Systems Security Program*. [online] Available at: https://inldigitallibrary.inl.gov/sites/sti/sti/3375141.pdf

[33] NCSD, 2009. *Common Cyber Security Vulnerabilities in Industrial Control Systems.* [online] Available at: https://www.us-cert.gov/sites/default/files/recommended_practices/DHS_ Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

[34] Piscitello, D., 2015. *Threats, Vulnerabilities and Exploits-Oh My*! [online] available at: https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my

[35] Zhu, B. and Shankar, S., 2010. *SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy*. [online] Available at: https://pdfs.semanticscholar.org/1027/2f29fff 747d7efccab3b58d64ffd1112c811.pdf?_ga=2.23427642.1638346716.1598251145-10156915 36.1558354618

[36] ENISA, 2011. *Protecting Industrial Control System. Recommendations for Europe and Member States.* Heraklion: The European Network and Information Security Agency.

[37] Byres, E., Kay, J. and Carter, J., 2003. *The Myths and Facts Behind Cyber Security and Industrial Control*. [online] Available at: https://www.controlglobal.com/assets/Media/ Media Manager/ The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

[38] Sullivan, J.E. and Kamensky, D., 2017. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal*, 30(3), 30-35.

[39] Newman, L.H., 2016. *What We Know About Friday's Massive East Coast Internet Outage*. [online] Available at: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

[40] Langner, R., 2011. Stuxnet: Dissecting a cyber warfare weapon. *IEEE Security Privacy*, 9(3), 49-51.

[41] Knapp, E.D. and Langill J.T., 2014. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. 2nd ed. Amsterdam: Elsevier.

[42] Katina, P.F., Despotou, G., Calida, B.Y., Kholodkov, T. and Keating, C.B., 2014. Sustainability of systems of systems. *International Journal of System of Systems Engineering*, 5(2), 93-113.

[43] Dewangan, B.K., Agarwal, A. and Venkatadri, M., 2019. Energy-aware autonomic resource scheduling framework for cloud. *International Journal of Mathematical, Engineering and Management Sciences*, 4(1), 41-55.

[44] Oberoi, P., Mittal, S., Gujral, K.R., 2019. ADRCN: A framework to detect and mitigate malicious Insider Attacks in Cloud-Based environment on IaaS. *International Journal of Mathematical, Engineering and Management Sciences*, 4(3), 654-670.

[45] Boppana, R.V. and Su, X., 2007. *Secure Routing Techniques to Mitigate Insider Attacks in Wireless Ad Hoc Networks*. [online] Available at: https://pdfs.semanticscholar.org/ 2885/ 0ddfbf73c09118fd8e14d1c6c1dc34141c74.pdf

[46] Omar, M., Mohammed, D. and Nguyen, V., 2017. Defending against malicious insiders: a conceptual framework for predicting, detecting, and deterring malicious insiders. *International Journal of Business Process Integration and Management*, 8(2), 114-119.

[47] Gao, J., Chai, S., Zhang, B. and Xia, Y., 2019. Research about DoS attack against ICPS. *Sensors*, 19(7), 1542, https://doi.org/10.3390/s19071542

[48] Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K. and Reddi, R., 2011. A control system testbed to validate critical infrastructure protection concepts. *International Journal of Critical Infrastructure Protection,* 4(2), 88-103.

[49] Morris, T.H. and Geo, W., 2013. Industrial Control System Cyber Attacks. *1st International Symposium for ICS & SCADA Cyber Security Research (ICSCSR)*, September 16-17, 22-29.

[50] Silberschatz, A., Galvin, P.B. and Gagne, G., 2013. *Operating System Concepts*. 9th ed. New Jersey: John Wiley & Sons.

[51] Varalakshmi, P. and Selvi, S.T., 2013. Thwarting DDoS attacks in grid using information divergence. *Future Generation Computer Systems,* 29(1), 429-441.

[52] Naoum, S., Chehab, A., Elhajj, I. H. and Kayss, I., 2013. Internal security attacks on SCADA systems. *Proceeding of the 3rd International Conference on Communications and Information Technology (ICCIT-2013): Digital Information Management & Security*, Beirut, 22-27.

[53] Naedele, M., 2007. Addressing IT Security for Critical Control Systems. *Proceedings of the 40th Hawaii International Conference on Systems Science (HICSS-40 2007): IEEE Computer Society*, Waikoloa, USA, 3-6 January, 2007, 40.

[54] Niland, M., 2003. *Computer Virus Brings Down Train Signals*. [online] Available at: http://www.informationweek.com/news/13100807.

[55] Roberts, P.F.Z., 2005. *PnP Worms Slam 13 DaimlerChrysler Plants*. [online] Available at: http://www.eweek.com/c/a/Security/Zotob-PnP-WormsSlam-13-DaimlerChrysler-Plants/

[56] Velagapalli, A. and Ramkumar, M., 2011. Minimizing the TCB for securing SCADA systems. *Proceedings of the 7th Annual Workshop on Cyber Security and Information Intelligent Research (CSIIRW'11)*, October 12-14, 2011. Article No.19, https://doi.org/10.1145/2179298.2179319

[57] Heckman, M., Schell, R. and Reed, E., 2011. Using a high assurance TCB for infrastructure security. *Proceedings of the 7th Annual Workshop on Cyber Security and Information Intelligence Research-CSIIRW*, October 12-14, 2011, Article No. 55, https://doi.org/10.1145/2179298.2179359

[58] Hewett, R. and Kijsanayothin, P., 2013. Securing system controllers in critical infrastructures. *Proceedings of the 8th Annual Cyber Security and Information Intelligence Research Workshop-CSIIRW*, January 2013, 1-4.

[59] Aesec, 2007. *GemSeal Guard*. [online]. Available at: http://aesec.com/guards/Aesec-GemSeal-SCADAConcept-070220.pdf .

[60] Azimi, M., Sami, A. and Khalili, A., 2014. A security test-bed for industrial control system. *Proceedings of the 1st International Workshop on Modern Software Engineering Methods for Industrial Automation- MoSEMInA*, New York, 2014, 26-31.

[61] Shahzad, A. and Musa, S.A., 2014. A review: Industrial control system (ICS) and their secuity issues. *American Journal of Applied Sciences*, 11(8), 1398-1404,

[62] Jie, P. and Li, L., 2012. Analysis of information security for industrial control system. *Process Automation Instrumentation,* 33(12), 36-39.

[63] Yasakethu, S. and Jiang, J., 2013. Intrusion detection via machine learning for SCADA system protection. *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*. Leicester, UK , September 16, 2013, 101-105.

[64] Valdes, A. and Cheung, S., 2009. Intrusion monitoring in process control systems. *Proceedings of the 42nd Hawaii International Conference on System Sciences*. Washington, DC., USA, January, 2009, 1-7.

[65] Drias, Z., Serhrouchni, A. and Vogel, O., 2015 . Analysis of cyber security for industrial control systems. 2015 *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, China, August, 2015, 1-8.

[66] Wang, X., Pang, L., Pei, Q. and Li, X., 2010. A scheme for fast network traffic anomaly detection. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, Taiyuan, China, 2010, V1-592-V1-596.
[67] Androulidakis, G., Chatzigiannakis, V. and Papavassiliou, S., 2009. Network anomaly detection and classification via opportunistic sampling. *IEEE/ACM Transaction on Networking*, 23(1), 6-12.
[68] Scheirer, W. and Chuah, M. C., 2008. Syntax vs. semantics: competing approaches to dynamic network intrusion detection. *International Journal of Security and Networks*, 3(1), 24-35.
[69] Chakraborty, S., Sarkar, S. and Ray, A., 2008. Symbolic identification and anomaly detection in complex dynamical systems. *Proceedings for the American Control Conference(ACC)*, Seattle, USA, 11-13 June, 2008, 2792-2797.
[70] Thottan, M. and Ji, C., 2003. Anomaly detection in IP networks. *IEEE Transactions on Signal Processing*, 51(8), 2191-2204.
[71] Tan, K. and Maxion, R., 2003. Determining the operational limits of an anomaly-based intrusion detector. *IEEE Journal on Selected Areas in Communications*, 21(1), 96-110.
[72] Liu, C.-C., Ten, C.-W. and Hong, J., 2011. Anomaly detection for cybersecurity of the substations. *IEEE Transactions on Smart Grid*, 2(4), 865-873.
[73] Debar, H., Marc, D. and Wespi, A., 2000. A revised taxonomy for intrusiondetection systems. *Annales Des Telecommunications*, 55(7-8), 361-378.
[74] Mitchell, R., & Chen, I.-R. (2014). *A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys*, 46(4), 1-29.
[75] Takano, M., 2014. ICS Cybersecurity incident response and the troubleshooting process. *Proceedings of the SICE Annual Conference*, Hokkaido University, Sapporo, Japan, 827-832.
[76] Conrad, E., Misenar, S. and Feldman, J., 2013. *Eleventh Hour CISSP*. 2nd ed. Amsterdam: Elsevier.
[77] Ning, P., Cui, Y. and Reeves, D. S., 2002. Constructing Attack Scenarios through Correlation of Intrusion Alerts. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washington, D.C., 2002, 245-254.
[78] Bartman, T. and Carson, K., 2016. Securing communications for SCADA and critical industrial systems. *69th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA, April 4-6, 2016, 1-10.
[79] Fielder, A., Li, T. and Hankin, C., 2016. Defense-in-depth vs. critical component defense for industrial control systems. *4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, Queen's Belfast University, UK, August 23-25, 2016, 1-10.