International Journal of Computer Engineering and Information Technology

VOL. 12, NO. 5, May 2020, 31–41
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

Industrial Control Systems (ICS): Cyber-attacks & Security Optimization

Erhovwosere Donald Emake[1], Ibrahim Adepoju Adeyanju[2] and Godwin Obruozie Uzedhe[3]

[1, 2] Department of Computer Engineering, Federal University Oye-Ekiti, Ekiti State, Nigeria

[3] Department of Electrical & Electronic Engineering, Federal University of Petroleum Resources, Effurun, Delta State, Nigeria

[1]emake.donald@fuoye.edu.ng, [2]Ibrahim.adeyanju@fuoye.edu.ng, [3]uzedhe.godwin@fupre.edu.ng

ABSTRACT

Cyber-security of digital industrial control system in reality is complex and challenging research area, due to various interconnections of electro-mechanical related components driving national critical infrastructures. These networked system components performs monitoring and controlling tasks in several industries and organization through the access of Internet connectivity across the world. More recently, there are myriad of security threats and attacks by malicious elements on ICS which now presents a priority to organizations and researchers for optimal security solutions. Development of the Internet and communication systems has also exacerbated such security concerns. Activities of cyber-attacks malicious elements on ICS may result in serious disaster in industrial environments, human casualties and loss. This paper critically looks at the SCADA/industrial control systems, architecture, cyber-attacks.. Other aspect of the paper examines current ICS security technologies including a computational secured algorithm for PLC.

Keywords: *ICS, SCADA, Cyber-Security, Cyber-Attack, Security Technologies.*

1. INTRODUCTION

The 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 electromechanical 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 within 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, 12]. Implementation practices of ICS systems have introduced a wide range of security vulnerabilities [13]. Presently there is a very high rate of vulnerability and cyber-attacks globally on ICS, some of these threats and attacking agents include terrorist network groups, dissatisfied employees, hostile governments and other malicious intruders [14]. Cyber-attacks consequences are very devastating with effects ranging from disruption or damage to critical infrastructural operations [15, 3] to significant effect on public health, safety, and destruction of lives and properties [14]. An in-depth understanding of the vulnerabilities, threats, and attacks are crucial to the defense mechanisms and security methodologies of any ICS environment.

Security threats on 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 technology that can serve as protection mechanisms.

2. INDUSTRIAL CONTROL SYSTEMS ARCHITECTURE

Each ICS has a process loop system of both electronic and mechanical components [9] to control the physical operations of machines. Figure 1 shows basic operation of industrial control system. Operator issues set-points commands from the Human-Machine Interface (HMI) to machines, either domestically in-plant or 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.

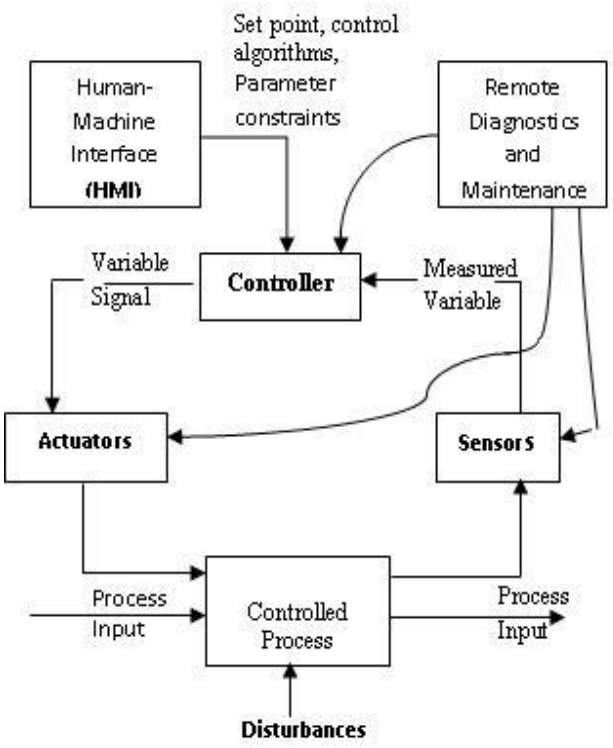

Fig. 1. ICS structure

Control Loop: Varied electronic/mechanical parts like sensors for measurement, controller hardware like PLC, actuators like control valves, breakers, switches, motors, and communication of variables are grouped as ICS control loop as shown in figure 1. 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 signals and generates the right processed variable output. The controller component access the issued set points commands from HMI, then transmits signal to the actuators, but the complete method changes with any slight disturbances which might lead to new detector signals been known to vary the state of the method in restraint.

Remote Diagnostics and Maintenance Utilities: This maintenance utilities is extremely very important in ICS operation, is designed to stop system failure when enabled. It additionally has the potential to spot and recover the system from varied failure modes. Varied technologies and applications are incorporated in it 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 system that enable operators to issue inputs commands that are translated as signals for machines that in turn give the specified result to the user. The HMI are employed for proper observation, configuration of desired set-point and adjusting control formula likewise establishing parameters within the controllers of an ICS.

2.1 Types of Digital Industrial Control Systems

In ICS operating environment, PLCs with different capabilities collaborate to attain various expected goals. Basic digital ICS commonly used in manufacturing, oil and gas industry and other Industrial environment [16] are clearly represented in figure 2. The diagram summarized the various types of ICS and their application:

Programmable Logic Controller (PLC): This is a skid mounted mechanism used for distinct control operation or specified application, providing restrictive control [17, 18]. 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.

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 production site; process parameters of the production plants are monitored and controlled with supervisory and regulatory control frame work within the working environment [19]. With several PLCs linked together as a distributed system, numerous tasks are effectively managed and performed. However, actual implementation

of ICS in industrial surroundings might typically be a hybrid of DCS and SCADA.

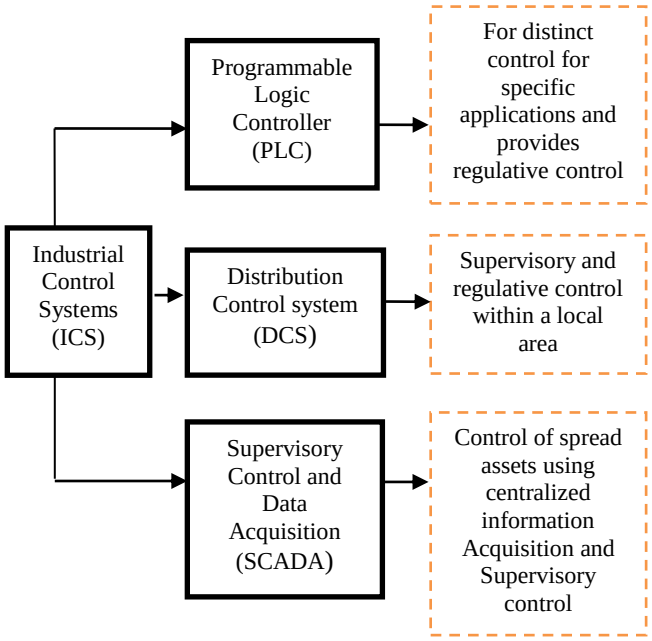

Fig. 2. Basic form of industrial Control Systems (ICS)

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 operation are often monitored and controlled from another location at a long distance, typically with wireless facilities connected to facilitate operations [20, 21]. SCADA reduces stress on staff from travelling to numerous operational remote sites when effectively deplored.

3. ICS CYBER-PHYSICAL ATTACKS

The control loop of a typical ICS constitutes industrial process application view which can be implemented following a hierarchy of industrial computing systems that make it vulnerable to threat attacking agents. The controller, which is usually known as the Programmable logic Controller (PLC) is a system that implements two logical processes: (a) it controls autonomously the connected devices at the lower level of the hierarchy, receives in input device information and controlling actuators (b) it further executes a part of a distributed application that controls the complete plant underneath the direction of the supervisory control and data Acquisition (SCADA) system, which acts with the SCADA system and presumably with different PLCs [22, 23]. ICS can therefore be said to be exposed to computational attacks and data attacks in a Cloud-based environment. Two basic types of attacks on ICS are internal/insider and external attacks [24].

Insider/Internal Attacks: This attack type leverages on the open platform in the Clouds. They are very dangerous and also harmful compared to external attacks. These attacks are caused by valid or legitimate users of Clouds. 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 calls for huge attention [25, 26]

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

3.1 Potential Cyber-attacks malicious element

This paper presents various malicious elements in human form and their operational attacking behavior on digital ICS. They include group of people such as hackers, script kiddies, industrial spies, terrorist, and even foreign armies and intelligence agencies [27]. Mentioned below are some Cyber-attackers groups.

Script kiddie: An attacker with malicious mindset who is inexperienced and unskilled probably found a security exploit and took up the courage using it to get reputation. This kind of attacker has rarely success in targeting protected systems, whether or not they initiate bulk of attacks currently faced by organizations.

Hacker: This could be a skilled attacker with huge knowledge of ICS operational environment that initiates attacks for gaining reputation in his locality. Hackers are very familiar with their target and may as well have good technical resource about their target. Generally, they establish attacking foresight from little knowledge about the target system architecture. Hackers usually target organization database to disrupt smooth operation of services rendered. They sometimes carry out their acts for monetary gain.

Disgruntled employee: This category incorporates a very high level of data about the plan targeted system. He/she initiates very dangerous attacks with access to internal industrial operations network; their input motivation is low and has reduced over time possibly due to lack of appraisal as laid down by the organization. He gradually

develops a biased unruly mindset to carry out revenge against his employer.

Terrorists: This is a group of persons with a very high malicious intention well-equipped with all available sophisticated software and hardware devices ready to launch attacks; they employ the services of skilled personnel with good resource level available at their disposal to carry out attacks. They work as individuals or as organized groups. Their motivation is for monetary gain and for spreading terror and clutter within society main critical infrastructures either to cause disruption in operation or harm workers operating such systems.
Industrial spy: These malicious persons try to induce access to confidential data or to sabotage the competition already existing in a particular industrial environment. They have very high knowledge and technical resources at their disposal to launch possible attacks, being specialists within the field; they are driven most often by decent gain motivation.

Cyber warrior: Is the most dangerous type among cyber attacks. These attackers have the very best levels of data, resources available to them to initiate possible cyber attack. The available data and resources becomes their motivational drive. They initiate and sustain distributed attacks on digital ICS whose networked components are exposed to the internet, such ICS components includes sensors, actuators and PLC, HMI etc, attacks associated with cyber warrior are dread and well coordinated against many targets simultaneously. Their sole objective is to interrupt or to destroy critical infrastructures. Cyber warrior is sustained by enemy countries within the context of electronic and knowledge cyber warfare.

3.2 Impact of Cyber Attacks on Industrial Control System Operations

Cyber-attacks on ICS environment depends on the target's nature of operation or the motivation of cyber criminals following the attack; impact could also be felt by a target's either internal or as external. The attacks can cause disruption by effecting changes in Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and alternative controllers. Like a modification in systems, a change in controller modules and alternative devices will result in broken equipment or facilities. Basically, this will additionally cause malfunction and disabled controls over a process. Common techniques of ICS cyber-attacks include the following.

- *Changes observed by altering system operations application configurations*: Once systems set-point data or vital parameters are altered, it's going to turn out unwanted or unpredictable results. This could be done to mask malware behavior or any malicious activity. This could also conjointly have an effect on the output of a threat actor's target.
- *Misinformation in line with operations:* False or misleading operational command could lead to implementation of unwanted or reserve actions owing to wrong knowledge. Such an occurrence might modify the programmable logic. This can jointly facilitate concealment of malicious activity, which has the incident itself or the injected code.
- *Alteration of safety controls procedures*: Forestalling the proper operations of safety measures can endanger lives of workers, and external clients might be put to risk.

3.3 Possible Consequences of ICS Cyber Attacks

Securing digital ICS is vital and compelling as business reliance on inter-connectivity increases on daily bases. However, Denial of Service (DoS) attacks and malware (e.g., worms, viruses) are becoming too common and have a direct impact on digital ICS. Cyber-attacks usually have physical and eventful effect. Consequential impacts of ICS attacks can be classified as follows [10].

Economic resultant Impacts: ICS incidents occur with a strong resultant physical impact. Physical impacts may result in repercussions to the system operations that in turn lead to a bigger economic sabotage on the production facilities, organization, or others 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 presumptive international economy.
Economic impact is categorized as second order impact in respect to its degree of assessment.
Social resultant Impacts: The consequences of this impact can result from the loss of public confidence in a company, with failed ICS due to cyber-attacks. Social impact consequences could be very unpleasant and dreadful. Social impact is categorized as second order impact degree of assessment.

Physical resultant Impacts: This type of impact underscores 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 regarding of degree of assessment.

3.4 ICS/SCADA device attacks classification

To undertake any security measures we must first understand the types of prevailing cyber attacks associated with a particular digital ICS and its environment. This becomes a fundamental requirement to militate against any cyber-threat attacks as key security measures. However to implement appropriate security framework we classify cyber attacks against ICS/SCADA systems into three (3) categories; which includes (i) ICS communication/network attacks (ii) ICS hardware and (iii) ICS Software attacks

Table 1: Cyber-attacks classification

ICS Cyber-attack Classification	***Attacking Mode***
ICS communication/Network Attack It encompasses all associated communication/network components including channel for data transmission.	• Cyber-attackers target the network layer, for example via the organization diagnostic server with a focus on the server UDP port. • At the transport layer attacker sends TCP connection requests faster than the machine can process using the SYN flood attack to saturate resources. • Attacks at application layer target various protocols used on ICS/SCADA system considering their low security capabilities to handle cyber threats e.g the DNS forgery/packet replay that is very are common in ICS application.
ICS hardware Attack PLC, actuators, sensors, and other ICS physical components	• Attackers clinch to false remote access to hardware components by altering operational data set points, this could cause devices to fail and remain at low threshold or rather change the alarm settings not to go off. • Lack of certification and documentation for administrative duties on ICS hardware components would give a well meaningful chance for attacker to reprogram the logic or set operational values to affect the functional behavior of the device.
ICS Software attacks IT applications/ICS embedded OS	• ICS/SCADA systems uses good numbers of software to supply the needed functionality from traditional IT applications which are customized into embedded device applications and inter-connected to HMI or Historian control applications. • VxWorks embedded Operating System (OS) a good example of embedded OS used in field devices; it provides minimum memory protection and support to the overall performance. • However, buffer overflow cyber-attacks are possible in such customized applications basically through workstations devices similar to standard IT systems or ICS automation software such as the historian servers. • Furthermore, field devices such as PLC that depend on real time operating systems (RTOS) are closely more susceptible to memory threat attacks by exploiting the allotted memory allocated time requirement in RTOS system. • ICS/SCADA components especially those integrity networks could be subjected to accumulated memory fragmentation that may result to what is known as programs stalling. • Structured Query Language (SQL) should be properly designed at the application layer level this is because it is widely used to store sensor data in historians and other databases. Poor design of SQL will eventually make the systems prone to SQL injection cyber-attacks. [28]

3.4 Demonstrating Cyber-Attacking Mode Vs Security Approach on ICS/SCADA Environment

Presented in this paper is a detailed and comprehensive analysis of current digital ICS/SCADA Cyber-attacks and best possible security technology designed to effectively handle current prevailing ICS Cyber-attack. It further, demonstrated various attacking mode by malicious elements (attacks agents) on critical components of digital ICS/SCADA systems. The three (3) major zones of ICS architecture [9, 29] as presented in figure 3 is exposed to an un-trusted environment. The diagram graphical illustrate how Cyber-attacks are carried out on each network ranging from production site/field site network, supervision/control network and corporate or enterprise network. An attack path (red dotted arrow line) is initiated by an external attacker who gained access through the

internet (EXT 1, EXT 2, EXT 3, EXT 4, EXT 5) ready to launch attack on the ICS/SCDA network architecture.
Every digital ICS environment may be surrounded with possible weaknesses or systems vulnerabilities depending on their individual configurations and their purpose. One fundamental determining factor for numbers of system vulnerabilities and cyber-attacks is seen on how big the ICS environment is and how un-secured its architecture network could be.

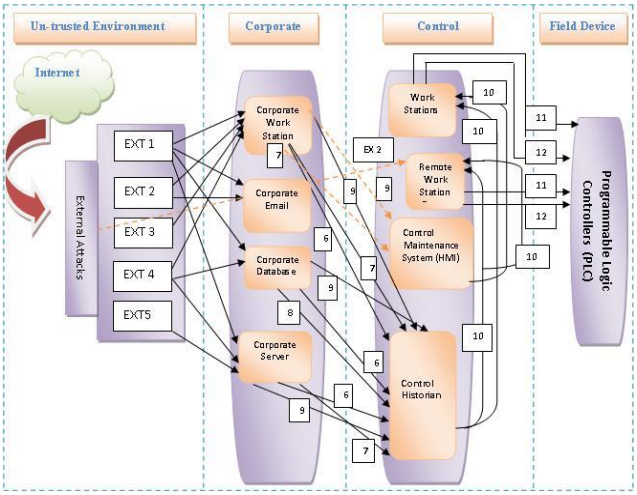

Fig. 3. Graphical illustration of Cyber-Attack path on ICS architecture

For an attacker having gained access through un-secured environment, simply launches malicious attacks through the internet to the corporate/enterprise network of the ICS architecture as indicated by the movement of arrow red dotted line to the sub-corporate network IT components such as the corporate work state, corporate emails, corporate data base and the corporate server.

Table 2: ICS architecture Cyber-Attack path graphical illustration table

ICS Attack Category	***Attackers technique***	***ICS targeted device***
Ext. 1	Internet Malware	Comm/Netwk
Ext. 2	Removable device driver Malware	Hardware
Ext. 3	Social Engineering	Software
Ext. 4	Malicious Remote Access	Software
Ext. 5	Cross site scripting	Software
Int. 6	SQL command Injection	Software
Int. 7	Authentication Bypass	Comm/Network
Int. 8	Removable device driver Malware	Software
Int. 9	Misuse of Access Authority	Comm/Network
Int. 10	LAN based Injection	Hardware
Int. 11	Buffer overflow	software
Int. 12	Man- in -Middle	Hardware

All possible attacks further launched from the corporate/enterprise network to the supervision/control network layer and production or field device network are group as internal/insider attacks which could be very deadly and dangerous, in the cyber-attack path such attacks are indicated in figure 3 in numerical numbers (6-12) and detailed description are outlined in table 2. The word INT in the table means internal/insider attacks.
The aim of most attackers is targeted on the production/field devices which play host to the ICS/SCADA Programmable Logic Controller (PLC) which is seen as the heart of the entire industrial operation. Every distributed Control systems (DCS) and Supervisory Control and Acquisition Data (SCADA) are inter connection of several PLCs with other ICS components (Hardware & Software) integrated together with several communication/network functional capabilities to drive critical physical infrastructure across the globe. Attackers sole objective is to disrupt functional services for monetary gain or otherwise or intentionally cause destruction of the system which could be harmful to field workers, control workers, office corporation staffs and largely to the entire community which may eventually leading to loss of life.

4. ICS SECURITY OPTIMIZATION

ICS security approach for Digital Industrial Control Systems has wide application in critical infrastructure across nations across the globe. Malicious attacks on ICS by threat agents can lead to serious consequences [26]. Therefore, a proactive security measure is an important factor to protect these critical infrastructures. In this section, current security technologies employed in Digital ICS environment to prevent and secure components from cyber-attacks are discussed. Generally, current ICS security technologies can be classified as Active Security Defense Technology (ASDT) or Passive Security Testing Technology (PSTT) as shown in Figure 4.

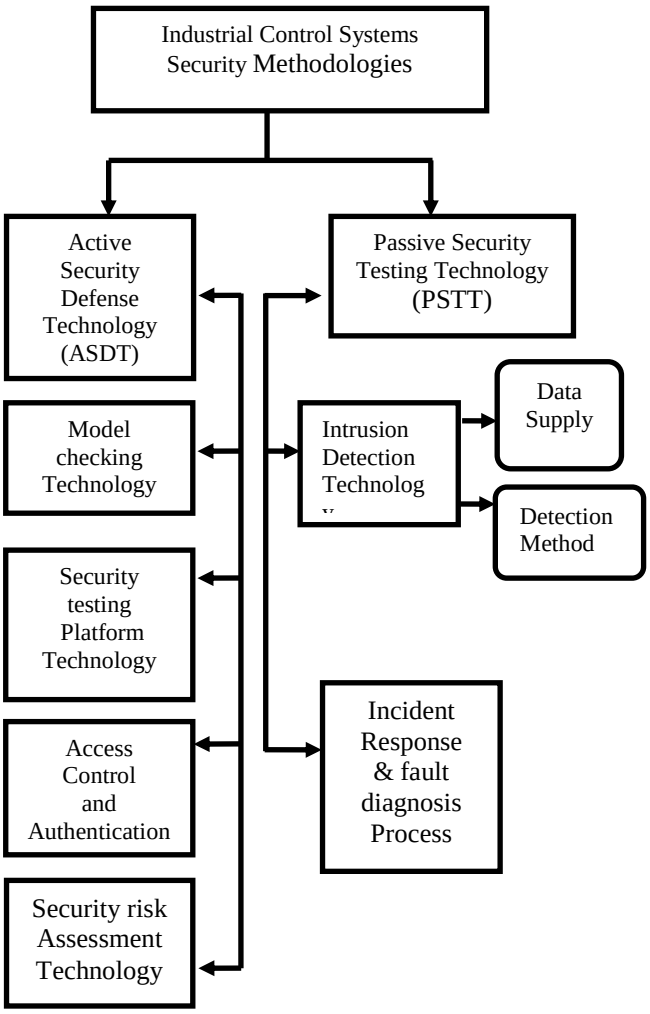

Fig. 4. Digital ICS Security optimization techniques

4.1 Active Security Defence 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 [30]. 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 Programmable Logic Controllers (PLC) that control industrial automation processes [31]. Additionally, the internet worm allowed attackers to gain total control of critical operation of a process plant from remote locations [32]. 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 [33].
The low complexness of STCB chips permits verification and building block of complicated trusted functionalities of system controllers [34]. However, this security approach assumes that everyone information from sensors and actuators don't seem to be impersonated by malicious attacks. 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 with considerable success recorded with a technique historically used for automated software package verification. The designed model was completely different from model-checking applications; it has the flexibility to uncover missing safety and security properties that ought to forestall catastrophes caused by malicious activities [33]

Security testing platform: Recent discovery on proliferation of cyber-attacks on ICS show that large number of security vulnerabilities exist in ICS. However, the ever-increasing rate of attacks on ICS results in the event of a security test-bed that became very crucial to evaluate the protection of ICS tools and products. One among such test-bed design security model is 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 platform, this platform covers all components of the ICS development and provides metrics for evaluations [35]. Also proposed was another security solution that uses cryptography implementations to protect the communication (SCADA/DNP3 protocol communication) and attacking scenarios that could be abnormal. This was based on existing and current SCADA/DNP3 associated security issues within each test-bed that was implemented [36]. 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 with the credentials readily available on database of licensed users or in a data authentication server. A form of distributed firewall that adds a protecting layer among internal subnet compared with traditional boundary firewall was used [37]. Its function is to make different configuration for each service object, it fully considered the running applications and network processing load when configured. Firewall rule configuration mechanism, which makes dynamic judgments of behaviour between control network and information network, was demonstrated. The spread of malicious code to other production equipment can be prevented by limiting inter-subnet communication strictly.

Security risk assessment: This introduces the concept of Security Assurance Level (SAL), which tries to measure

the security of an ICS with the norm methods. It can be used by users of the ICS

4.2 Passive Security Testing Technology

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

Intrusion Detection Technology: Intrusion detection is a passive security defence strategy that observes and analyses the events taking place in an information system with the aim of discovering signs of security issues [38]. For ICS systems, intrusion detection is network behaviour through the gathering and analysis of system information [39]. This security technology detects whether there is invasion against digital ICS systems by constantly comparing with known intrusion model or making decision and analysis for the unknown intrusion model [6]. Therefore, new detection rules and observance mechanisms are created specifically for ICS systems and networks taking into consideration the designed specification of communication protocols. These new rules in the designed model are mainly based on attack signatures, anomaly detection, probabilistic models, system specifications as well as the behaviour of ICS components [40]. Iterative estimation of Hurst parameter for rapid detection, opportunistic samplings for classification of anomaly detection, and network intrusion detection with semantics-aware capability have been previously proposed [41, 42, 43]. Also, a data-driven technique based on the concept of symbolic dynamics and information theory has been described [44]. Detection of network anomalies was proposed using statistical technique; the mechanism was called signal processing approach [45]. An operational limits and effectiveness was also proposed to conclude an intrusion [46, 47]. To perform its task effectively, the intrusion detection system (IDS) uses different data sources from the monitored ICS environment. The IDS through a detection methodology detected the presence of an intrusion and raised an alert. Classification of IDS is determined by the type of information source and the detection methodology used [48]. Insight on the effectiveness of IDS techniques application on digital ICS is established on two design and classification approach namely the detection approach and the audit material approach [49]

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 infrastructure. Mis-configuration, human error, failure, and attackers target ICS to lose availability and integrity [6]. Improvement level of industrial control system emergency response and fault diagnosis ability helps further protection of the safety of industrial control system. ICS network security incident response and troubleshooting process was proposed to improve security concern [50]. Security incident on ICS could be a harmful occurrence on a system or network. The goal of the incident response set up is to permit the organization to manage the cost and injury related to incidents and to form the recovery of the cost systems faster [51].

4.2 Depth Defence Strategy

Overall, complete digital ICS security cannot be achieved solely on a single security technology solution. Therefore, it became imperative to integrate a range of security technologies hierarchically to boost the defence capability of industrial systems. The United States Department of Home Security [52] proposed a "defense in depth" strategy; the model is segmented into five (5) layers. The first layer is the use of commercial firewalls; deployment and use of firewall, intrusion detection, vulnerability scanning and other proactive security measures can be helpful in militating against possible ICS attacks acting as an integral protection [52, 53]. Man-in-the-Middle attacks can be averted by securing field device by deploying and safe guarding the environment using field level firewalls designed for PLCs, IEDs, and SCADA RTUs [54]. Second layer is the joint security approach to defend 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. Fourth layer is the monitoring of field devices while security log management and data backup is taken care of by the fifth layer.

4.3 Programmable Logic Controllers (PLC) Security Optimization algorithms using Fuzzy Logic

To achieve a better approach to secure PLC operational set-point, this paper proposes a computation algorithm that could improve controller's security strategy from possible cyber-attacks by malicious element if properly designed. It is an integrated security solution for both PID and FL controllers for the purpose of securing ICS/SCADA from threat actor.

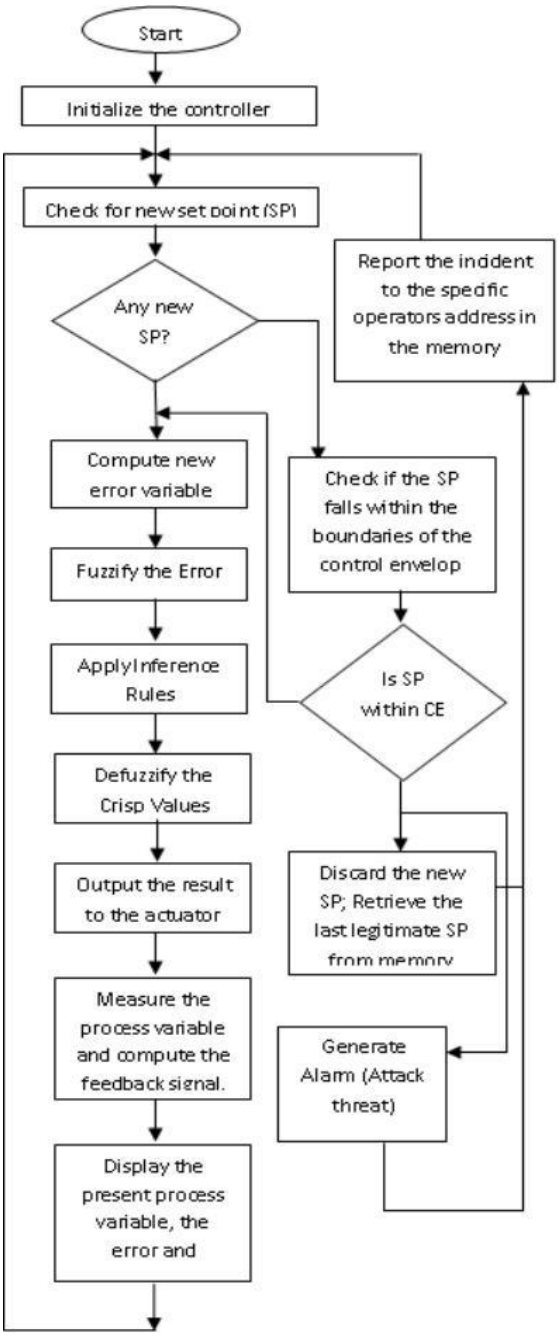

Fig. 3.4 High level flow chart for the proposed model

5. CONCLUSION

ICS security is currently of most importance to organization assets owners and researchers as a result of the present wave of malicious cyber attacks on ICS/SCADA system across the globe. Therefore integrating security features in field device component such as the Programmable Logic Controller (PLC) that drives critical infrastructures is of great concern, not only can such security solution improve operation at production site, management level, but can also ensure safety/security and reliable production thereby preventing consequential harmful effect that could result from possible unexpected cyber-attacks. Presented in this paper are some security technologies that are currently applicable in securing ICS/SCADA systems. However the development of fuzzy logic controllers with integration of a computational security algorithm model at the back-end ICT solution for Control System (CS) could help to provide better and improved ICS/SCADA security operation.

REFERENCES

[1] A. Coletta, and A. Armando, "Security monitoring for Industrial Control Systems". Proceedings of the 1st Conference on Cybersecurity of Industrial Control Systems and the First Workshop on the Security of Cyber Physical Systems, WOS-CPS, Vienna, Austria, 2015, pp. 48-62.

[2] Y. H. Hu, et al.. "A survey of intrusion detection on industrial control systems", International Journal of Distributed Sensor Networks, 2018, Vol. 14, No. 8.

[3] F. Obodoeze, F. N. Obiokafor, and T. Asogwa,. "SCADA for National Critical Infrastructures: Review of the Security Threats, Vulnerabilities and Countermeasures", International Journal of Trend in Scientific Research and Development(IJTSRD), Vol.2, No. 2, 2018, pp. 974-982.

[4] J. Weiss, "Protecting Industrial Control Systems from Electronic Threats". First edition, New-York, Momentum Press, 2010 pp 1-310.

[5] M. Hentea. "Improving Security for SCADA Control Systems", Interdisciplinary Journal of Information, Knowledge, and Management, Vol. 3, 2008, pp 73-86.

[6] X. Fan, K.. Fan, Y. Wang, and R. Zhou, "Overview of Cyber-security of Industrial Control System", International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC), 2015. Pp.1-7.

[7] A. A. Cardenas, S. Amin and S. Shankar, "Research challenges for the security of control systems". Proceedings of the 3rd conference on Hot topics in security, Vol. 6, 2008, pp. 1–6.

[8] P. Uchenna, D. Ani, M. H. Hongmei and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure; manufacturing inperspective", Journal of Cyber Security Technology,Vol. 1, No. 1, 2016, pp 32-37.

[9] Stouffer, Falco and Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82 Revision 1, 2013. http://dx.doi.org/10.6028/NIST.SP.800-82r1

[10] K. Stouffer, V. Pillitteri, M. Abrams and A. Hahn, "Guide to Industrial Control Systems (ICS) Security", NIST Special Publication 800-82 Revision 2, 2015. http://dx.doi.org/10.6028/NIST.SP.800-82r2

[11] C. Alcaraz and S. Zeadally, "Critical Control System Protection in the 21st Century", Computer Vol. 46, No. 10, 2013, p. 74–83.
[12] B. Miller and D. Rowe, "A Survey of SCADA and Critical Infrastructure Incidents". Proceedings of the 1st Annual conference on Research in information technology, 2012, pp 51-56.
[13] A. Sajid, H. Abbas and K. Saleem, "Cloud Assisted IoT-Based SCADA Systems Security". A Review of the State of the Art and Future Challenges, IEEE Access 4, 2016, pp 1375–1384.
[14] A. Radvanovsky and R. McDougall, "Critical Infrastructure: Homeland Security and Emergency Preparedness", Second Edition. Boca Raton, CRC Press, 2009, pp 1-318.
[15] O. A. Hathaway et al., "The Law of Cyber-Attack. California Law Review", Vol. 100, No. 4, 2012, pp. 817-885.
[16] T. Lu, X. Guo, Y. Li, Y. Peng, X. Zhang, F. Xie and Y. Gao, "Cyberphysical Security for Industrial Control Systems Based on Wireless Sensor Networks", International Journal of Distributed Sensor Networks. Vol. 10, No. 6, 2014, pp 1-17.
[17] A. R. Kiran, B. Sundeep, S. C. Vardhan and N. Mathews, "The principle of programmable logic controller and its role in automation". International Journal of Engineering Trends and Technology, Vol. 4, No. 3, 2013, pp. 500-502.
[18] C. Wang, M. X. A. Liu and J. Zhang, "The Application of PLC Control System in Oil and Gas Pipeline Transportation". Proceeding of the 2nd International Conference on Mechanical Control and Automation (ICMCA), 2017,
[19] S. Anand, S. Sarkar and S. Rajendra, "Application of distributed control system in automation of process industries", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, No. 4, 2012, pp 377-383
[20] T. H. Kim,"Integration of Wireless SCADA through the Internet". International Journal of Computers and Communications, Vol. 4, No. 4, 2010, pp. 75-82.
[21] D. O. Kovaliuk, K. M. Huza and O. O. Kovaliuk, "Development of SCADA System based on Web Technologies", International Journal of Information Engineering and Electronic Business (IJIEEB), Vol. 10, No. 2, 2018, pp. 25-32
[22] P. F. Katina, G. Despotou, B.Y. Calida, T. Kholodkov and C. B. Keating , Sustainability of systems of systems . International Journal of System of Systems Engineering, Vol. 5, No.2, 2014, pp 93-113.
[23] NIST, Framework for Cyber-Physical Systems. National Institute of Standards and Technology (NIST) Special Publication 1500-201, Vol. 1, 2016, pp 11-38
[24] R. V. Boppana, and X. Su, "Secure routing techniques to mitigate insider attacks in wireless ad hoc networks". IEEE Wireless Hive Networks Symposium 200, 2007.
[25] M. Omar, D. Mohammed and V. Nguyen, "Defending against malicious insiders: A conceptual framework for predicting, detecting, and deterring malicious insiders". International Journal of Business Process Integration and Manage ment, Vol. 8, No. 2, 2017, pp 114-119
[26] J. Gao, S. Chai, B. Zhang, and Y. Xia, "Research about DoS Attack against ICPS. Sensors", Vol. 19, No. 7, 2019., pp 1542.
[27] E. Pricop and S. F. Mihalache, "Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems". 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2015
[28] B. Zhu, A. Joseph and, S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems", International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp 380-388.
[29] A. Fielder , T. Li and C. Hankin, "Defense-in-depth vs. Critical Component Defense for Industrial Control Systems" 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR), 2016, pp 1-8
[30] M. Naedele, "Addressing IT Security for Critical Control Systems", Proceedings for the 40th Hawaii International Conference on Systems Science (HICSS-40 2007), IEEE Computer Society, 2007, pp 40
[31] M. Niland, "Computer Virus Brings Down Train Signals" [online] Available at: http://www.informationweek.com/news/13100807.
[32] P. F. Z. Roberts, "PnP Worms Slam 13 DaimlerChrysler Plants". 2005 [online] Available at: http://www.eweek.com/c/a/Security/Zotob-PnP-WormsSlam-13-DaimlerChrysler-Plants/
[33] A. Velagapalli and M. Ramkumar, "Minimizing the TCB for Securing SCADA Systems", Proceedings of the 7th Annual Workshop on Cyber Security and Information Intelligent Research (CSIIRW'11), No.19, 2011
[34] M. Heckman, R. Schell and E.. Reed, "Using a high assurance TCB for infrastructure security", Proceedings of the 7th Annual Workshop on Cyber Security and Information Intelligence Research – CSIIRW, 2011, No.55,
[35] M. Azimi, A. Sami and A. Khalili, "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, pp. 26-31.
[36] A. Shahzad and S. A. Musa, "A review: Industrial Control System (ICS) and their secuity issues". American Journal of Applied Sciences , Vol. 11, No. 8, 2014, pp 1398-1404,
[37] P. Jie, and L. Li, "Analysis of Information Security for Industrial Control System. Process Automation Instrumentation, Vol. 33, No. 12, 2012, pp. 36-39.
[38] S. Yasakethu, and J. Jiang, "Intrusion Detection via Machine Learning for SCADA System Protection. Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research, 2013, pp 101-105.
[39] A. Valdes and S. Cheung, "Intrusion monitoring in process control systems". Proceedings of the 42nd Hawaii International Conference on System Sciences, 2009, pp 1 - 7.

[40] Z. Drias, A. Serhrouchni and O. Vogel. "Analysis of cyber security for industrial control systems", Proceedings for the International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC}, Shanghai, China, 2015, pp 1-8.
[41] X. Wang, L. Pang, Q. Pei, and X. Li, 2010, "A scheme for fast network traffic anomaly detection". Proceedings for the International Conference on Computer Application and System Modeling (ICCASM), Taiyuan-China, 2010, Vol. 1, pp. 592 –596.
[42] G. Androulidakis, V. Chatzigiannakis and S. Papavassiliou "Network anomaly detection and classification via opportunistic sampling". IEEE/ACM Trans. Network, Vol. 23, No. 1, 2009, pp. 6 –12.
[43] W.Scheirer and M. C. Chuah, "Syntax vs. semantics: competing approaches to dynamic network intrusion detection, Int. J. Security and Networks, Vol. 3, No. 1, 2008, pp 24-35
[44] S. Chakraborty, S. Sarkar and A. Ray, "Symbolic identification and anomaly detection in complex dynamical systems". Proceedings for the American Control Conference(ACC), Seattle, WA USA, 2008, pp. 2792 -2797.
[45] M. Thottan and C. Ji, "Anomaly detection in IP networks", IEEE Trans. Signal Process,Vol. 51, No. 8, 2003. pp. 2191 -2204
[46] K. Tan, and R. Maxion,, "Determining the operational limits of an anomaly-based intrusion detector". IEEE J. Sel. Areas Commun, Vol. 21, No. 1, 2003, pp. 96-110.
[47] C.-C. Liu, C.-W. Ten and J. Hong, "Anomaly detection for cybersecurity of the substations". IEEE Trans. Smart Grid, Vol. 2 No. 4, 2011, pp. 865 –873.
[48] H. Debar, D. Marc and A. Wespi, 2000. "A revised taxonomy for intrusiondetection systems". Annales Des Telecommunications, Vol. 55, No. 7-8, 2000, pp. 361–378.
[49] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems ». ACM Computing Surveys, Vol. 46, No. 4, 2014, pp. 1-29.
[50] M. Takano, "ICS Cybersecurity Incident Response and the Troubleshooting Process", SICE Annual Conference, Sapporo, Japan, Hokkaido University, 2014, pp. 827-832.
[51] E. Conrad, S. Misenar and J. Feldman, "Domain 7: Operations Security. Eleventh Hour CISSP". Eleventh Hour CISSP, 2014. pp. 117–133.
[52] DHS, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, Control Systems Security Program". Dept. of Homeland Security, National Cyber Security Division, 2009. [online] available at: https://inldigitallibrary.inl.gov/sites/sti/sti/3375141.pdf
[53] P. Ning, Y. Cui and D. S. Reeves, "Constructing Attack Scenarios through Correlation of Intrusion Alerts". Proceedings of the ACM Conference on Computer and Communications Security, Washington, D.C., 2002, pp. 245-254.
[54] T. Bartman and K. Carson, "Securing communications for SCADA and critical industrial systems", 69th Annual Conference for Protective Relay Engineers (CPRE) College Station, TX, USA, 2016.