ISSN 2047-3338

Security Challenges of Industrial Communication Protocols: Threats, Vulnerabilities and Solutions

Khalid Imtiaz[1] and M. Junaid Arshad[2]

[1,2]Computer Science and Engineering Department, University of Engineering and Technology, Lahore, Pakistan

[1]engr.khalidimtiaz@gmail.com

***Abstract*– Industrial communication protocol (ICP) is used in order to exchange the data among the Industrial management system and field side instruments. By the intensity integration of industrialization, informatization and the speedy advancement of the internet, the ICCPs (Industrial Control Communication Protocols) dangers becomes progressively more outstanding. The industrial and domestic communication protocols show huge similarity between them. The hierarchy at the upper level of both domestic and industrial networks is same this is the reason that researchers are still looking for the development of the best Industrial Communication Protocols (ICPs) by proposing or suggesting the new techniques or architecture for the domestic communication protocols. In this research work, we present the security challenges and present standard's issues control industrial communication frameworks, just like Modbus RTU/ASCII, Foundation fieldbus, CAN OPEN, Open Platform Communications etc. At that point the security suggestions are raised up against these kinds of problems. The wellbeing of entire controlled communication system may be enhanced just by enhancing security of the correspondence conventions. The main focus of our research is to discuss the security challenges, threats and vulnerabilities of industrial communication protocols and then provide their possible solutions, as it is required for conventional industrial communication protocols towards the improved modern high-speed Industrial control system (ICS).**

***Index Terms*– Industrial Control System, Industrial System Automation, Industrial Communication Protocols, Vulnerabilities, Threats, Security Challenges, IDPS and Modbus Protocol**

I. INTRODUCTION

MODERN control framework (ICS) is an essential foundation of a nation associated with electric power, vitality and numerous different zones of individuals' occupation. ICS has been utilizing complex restrictive correspondence conventions, for example, Modbus, profibus, ICCP, IEC, OPC, DNP3 and so on, these correspondence conventions finish the ICS information trade and obtaining, business observing and numerous other imperative capacities. Be that as it may, with the profundity mix by industrialization and informatization and the fast improvements made by the Web, which have been neglected by the security issues to be progressively unmistakable. Right from the starting of 1980s the industrial communication systems are being used. Till to date, great changing has been done in the technologies as new ideas were required to meet the new demanding requirements. The devices which are in use today are breaking all the traditional viewpoints of the automation pyramid. The CPUs are getting smaller and faster and the sensors are being improved and great advancements are done in the field of intelligence of the computers. The term of "Smart Instruments" have been used for these devices which are the intelligent devices. The smart instruments can also include important hardware which have to be directly joined within the control levels of the automation pyramid, which in fact mix up with the classic definition of the levels. Hence, it is very important to differentiate between the operational architecture and the functional architecture.

The F secure (the security merchant) have found the havex infection in June 2014. It exploited the social building to send data requiring messages that contains the vindictive spy-ware to the objective clients, and as the clients take programming which is altered, this malevolent code of spy-ware was consequently introduced to OPC customers for information by means of OPC convention [11]. This demonstrates the security of the ICS conventions is exceptionally stressing. Advanced controllers started to persistently simple manipulate, though, the information transfer to the field was still achieved by simple tools. Implementation of advanced frameworks was carried out for the requirement of new conventions of the correspondence to the field in addition among the controllers [12].

The convention of the correspondence is usually referred as fieldbus conventions. Industrial network controlling elements: Industrial communication and control frameworks are including of special equipment and functions, like Supervisory Control and Data Acquisition Systems (SCADA), Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS). That is used for communications between the field devices and framework control application. Thus, this paper highlights the Security Challenges of Industrial Communication Protocols: Threats, Vulnerabilities and Solutions. It presents an IDPS solution on heterogeneous Industrial Control system, constructs a calculation mode for threats detection and points out the general framework for

Vulnerabilities prevention which provides the basis for the RTSP (Real-Time System Protection). Industrial Control systems have a lot of application domains that include batch, discrete and process manufacturing. Process manufacturing includes generation and distribution of electric power, supply of water and gas and the transportation. The elements are dispersed on a local, wide-area or the global gage and this is done on the basis of type and purpose of central system. The most important element of the distributed control systems are communication links and facilitates and these are also discussed in many papers of this very issue.

In the past Industrial Control systems were not connected with the public networks and with each other. Now the companies are being pressurized to make co-effective and fast decisions. To achieve this purpose up-to-date and accurate information is required. This information should be about the plant and status of process that should be available at the management level as well as the plant floor. As not much Research work done in the area of Industrial control communication protocols which is greater demand of modern-day industry this thing motivates me to do research on the comparative analysis of different industrial communication network protocols on basis of their characteristic, transmission mechanism and performance.

II. LITERATURE SURVEY

The functions of administration systems of industry are composed of fieldbus protocols that are categorized in IEC standards rule 61158 as a computer control, multipoint, series of, data transfer for the communications within the industrials framework & field side instruments, for example yet not constrained to signal converter, control valves and nearby control systems. The initially fieldbus was used as the reciprocal of the two-wire conventional flagging strategies such as, Conventional industrial controls signal are 4-20ma and 0-10V; the modern era improvement has extended and now more upper level control signals establishment.

The core of disbursed automation structures is largely the dependable trade of statistics. Any attempts to steer techniques in parallel of non-stop human interaction requires, in a completely extensive experience, the glide of data between a few sorts of actuators, sensors & controllers [1], after the steam energy advent to alleviate people from hard guide to hard work & the invention of mass productions based totally on department of labors, creation of automation technologies turned into what's nowadays frequently known as the 0.33 business revolutions. To help facts exchange, a large number of industrials conversation network developed over the years, stars from the Nineteen Eighties. Ethernet, Wi-Fi networks, or Internet technology are the good example of these cross-fertilizations.

Such newly technologies generated newly opportunities for making information alternate more comprehensive. As a result, automation structures should develop extra complicated, too. The today's trends influencing automation era are CPS, IoT. For the latter [2], explain industrial control system automation as the major, steadily developing software discipline, those standards are not totally emerged & new in the context of ICT many years in the past, as they are penetrating industrial automations & converting the angle from which people observe automations structures [3]–[5]. Furthermore, they aid latest traits, along with achieved a better degree of interconnections; cognitive automations, & transferring information collections & processing in to cloud-primarily based programs [6]–[8]. Making use of ideas of IoT & CPSs to the economic automations area brought about the definitions of the industries 4.0-idea, in which 4.0-alludes to a 4th industrial revolutions enable by net technology for the creation of clever products, smart services and clever production. Initially progressed in Germany, the time has fast come to be a slogan on an international scale [10]. In the response with the same goals, (IIC) commercial internet initiative initiated in the U.S., however it has to be considered that the time period became coined lots quicker [11]. As from the communications viewpoint, CPSs and the IoT depend in large part on net of cell, such as the telecommunication networks, which do no longer have a very great function in communication within the industries to this point. As an addition, they require communications which are exclusively dependent on the internet, which has not been feasible in automation of the business, either both Telecom Networks and Information Technology (IT) could not really deal as the automation-particular desires for deterministic, efficient and reliable verbal exchange. On the individual hand, current paintings on TSN Ethernet guarantee solid immediate abilities, which are visible as real sport changer for the immediate automation networking.

Then again, telecom industries have determined business automation as a promising utility discipline in their merchandise and appears decided to do not forget the wishes of improve their automation of 5G networks. Both tendencies, together with semantic and unified statistics demonstrating primarily based as web requirements, would possibly unquestionable alternate of the business structure, and they could be acting as the prerequisite for in reality imposing industrial CPSs and IoT. Research work is done for the few and a long what critical enhancements of fieldbus frameworks, more often by individual researcher personally involved in the progression or institutionalization forms. Advancements in the modern control system will be demonstrated in this segment, however, the check is advised to mention the stepwise history (Table I).

III. PROBLEM STATEMENT AND RESEARCH OBJECTIVES

Due to industrial revolution, the security threats and vulnerabilities of Industrial Communication Protocols have become a great challenge, so that it is needed to address these issues by proposing the reliable security solutions to safe Industrial Control Systems (ICSs).

Modern Industrial Control Systems (ICS) required better and improve communication protocols. Industrial communication Protocols (ICP’s) like Profibus, CAN open, Modbus Serial/RTU, Control Net Protocol, Device Net Communication, Foundation Field Bus and ASI having Issues (such as GUI, Security Issue, Cost effectiveness, Lake of Diagnostic Features etc.) demand proper solution by proposing a new approach/framework for ICPs. By doing this, it can be capable to fill the research gaps.

Table I: Comparison of Existing ICS Security Techniques

Sr. No	Reference	Techniques/ Framework	Purpose	Performance / Accuracy
1	Fleury. et al, 2012 [15]	Vulnerability as exploitable weakness	Identify areas of weakness to facilitate mitigation Planning	67.5 % (Accuracy)
2	Fleury. et al, 2013 [14]	Attack-vulnerability-damage model	Serve as a precursor to a full developed taxonomy to provide a comprehensive understanding of cyber-attacks against ICS in the energy critical infrastructure sector.	Achieved good accuracy.
3	Zhu. et al, 2014 [13]	A taxonomy of targeted attacks	Education and for prioritizing preventive measures.	72.1 % (Accuracy)
4	Line. et al, 2015 [12]	Taxonomy of cyber-attack on SCADA System	Identification and classification of potential cyber- attacks on SCADA System including cyber physical attacks.	75.2 % (Accuracy)
5	Smith. et al, 2016 [11]	A Proposed taxonomy for vulnerabilities	Provide a framework to access countermeasures currently available to protect ICS systems.	76.8 % (Accuracy)
6	Oltramari. et al, 2017 [10]	Ontological approaches to SCADA vulnerabilities or attacks	Use semantic language to capture structural relationships among systems and vulnerabilities for use as an incident analytic tool, forensic analysis and mitigation planning.	78.3 % (Accuracy)
7	Fleury. et al, 2018 [9]	Cyber attacker taxonomy	Increase awareness of categories of attackers in ICS cyber incidents, can be used to complement other taxonomies.	81.5 % (Accuracy)
8	Flower. et al, 2019 [8]	Incident-based matrix	Provide an integrated approach to viewing cyber incidents.	82.7 % (Accuracy)

To meet the modern industrial requirements, ICPs have to improve the standards used to determine how data transmission on communication network devices, Programmable logical controllers, Desktop PC's, and so on. With better development structures of ICPs, it can be ensuring that less time required for data transfer, secure data transmission, and reliable time synchronization, and real-time deterministic response in some control process and applications. Industrial control communication protocols (ICCPs) also responsible for sending information reliably without bugs and securely between nodes on the communication control network. Due to all above factors and modern industrial system requirement a comprehensive performance analysis of ICPs is required to resolve the problems in existing ICPs.

IV. THREATS AND VULNERABILITIES OF INDUSTRIAL CONTROL SYSTEM

Vectors of Threats

There are several methodologies which are being used by the attackers for the achievements of the very unauthorized admission into the critical system. The paper discusses that multiple threat vectors can be used for this very reason. The threats vectors can only be stopped when they are understood and studied thoroughly. A few numbers of vectors should be understood for the assurance of the appliance of the very best and appropriate security measures.

A) Replay Attack

The replay attack is initiated with a user intercept that is malicious, the access to the communications of the store so that these communications could be reused and the captures of the communications, such as, as soon as the attacker encounters with a trial for the password, the complaint would be sent to the store owner at that very moment. If we take other examples it is said that the attacker may also receive the communication which is streamed wirelessly on the SCADA device and can use that communication for the later use. This type of the attack does not need a very thorough studies on the communication or on the communications protocols, such as, if a breaker open command is captured it could be use regardless of its encryption. If the proper justification is used, the message which is used as the replay may be acted as legitimate as it could be used for the control or the unauthorized access to the communications.

B) Brute Force Attack

The password as well as the data which is encrypted could be targeted by the help of the attack of brute force. The data which is encrypted could be open if the password is decoded by using all the attempts of the possible key combinations. The uprising of this attack is being reported by the ICS-CERT, back in February 2013, and it shows that this attack is used as much as the critical level [3].

C) Dictionary Attack

The password could also be broken by the utilization of the attack named as the dictionary attack. This method can break the password only if all the predefined list of passwords is being tried which are present in the form of a very long term.

D) Eavesdropping

The attack known as the Eavesdropping could be done by using several forms. It may be possible that some of the techniques used may appear as the high-end techniques, but the use of simple techniques may have more lasting and effective techniques. The information about the network is very much important if the attacker is going to attack on the SCADA system [4].

E) Denial-of-Service Attack

The DoS attack is being done for the delaying of the services which are being available for the utilization. The requests have been flooded in this technique in abundance by the help of which the network is being saturated which causes the delay in the travel of the legitimate request in the network system. The main target of the DoS attack is the grid system which is basically the electric power [4]. However, the DoS attack is not only limiting its circle to the data flooding. The attack is not just the data flood but the DoS attack.

F) Mitigation Techniques

The main purpose of the security plan used is to basically the reduction of the risk to the network system. In the sections discussed above shows that there are multiple ways to attain the access, the execution of the malicious activities and the attainment of the intelligence. The attack of each type has been in the technique which is the mitigation technique. The relay attack is been recalled with the help of the intercepted password with the help of the command which is controlled in the way of the encrypted replayed. With all the packet sent there will be the numerous sequences, and this is done by the help of the protocol which is the IPsec. These are the systems which are being used for the attack known as the replay. The man in the middle is the similar technique as the mitigation technique. The authentication is the key complement for the accomplishment of this defence system. The authentication incorporated with the strong encryption is used for the provision of the defence. For several type of attacks, the most adequate methods for the provision of the defence and it is also mentioned in the 3rd section. The data modification is also being relied on the authentication.

G) Mitigation Controls

The authentication with the help of the encryption is being known as the first step to squeeze down the communication in the functionality of the mitigation. Above, it is being discussed that the encryption is not being known as the tool for the prevention of the data as well as the prevention from the replay attack. In the segment of the utilities of the engineering the Dial up modems are being used at a very scale for the accession remotely [11]. By these the presence of the unauthorized access is being shown or risked. The identification of the modems is being done by the help of the war dialler software by the attacker or the hacker. So, basically the best method is the disconnection of the modem which is not being used at a very specific time period. Phone calls are also being used for the accession to the modem as well and this require a very short number of the utilities. The modem is being switched in the modem manually shortly after the access is being granted. The passwords which are weak in nature are also being used for the attack on the password and for these the brute force attack is being used as the dictionary. As the password is being set on the default set by the factory the breaches are being done with in the physical devices were made successfully. These types of the passwords are being known by the attacker and it is also known as the fair assumption to this extent. So, to prevent these types of breaching one must change the password from the default password set by the factory and configure a new and a strong password for the system. The case for the characters, low number of the characters and the symbol is being required. Or the proxy must be set for the device if the device does not support such type or length of the password [11]. A strong tunnel is also being used between the user and the server for the better protection of the password, hence, device or network.

V. CHALLENGES AND NEW SECURITY SOLUTIONS

There are some very major differences in the grid networks which makes it hard for the traditional security solutions to work on them. The security objectives are different in these grid networks in such a way that in thee IT network security systems three objectives are under the observations which includes the integrity, confidentiality and the availability whereas in the grid networks aims are the provision of the equipment, human safety and the protections of the power line as well. Furthermore the grid network architecture is far different than the IT network as in the IT networks the security act as the archiving and providing critical protection to the center of the IT network which is the place where the information reside, and the protection protocols followed in the grid network are done on the edges as well as the center of the system. Lastly the QoS which is commonly known as the quality of the service metrices are of different kind in the IT networks for the reinitiating of the devices in the case of the update or the failure, moreover it is not the very acceptable kind of thing in the case of the grid networks because the services should must be online at all the time. All the major differences which are being discussed above between the grid networks and the IT networks securities there is a very acute need of the security solutions which are only be applicable on the smart grid networks. There are certain challenges in the development of the security solutions for the grid networks and some of these are as follow:

- There are some components in the grid networks which are not being controlled by the security rather than that they are being controlled by the propriety OS.
- The design of the automation system was not comprising the component of the security at all.
- The security in the system should be combined with the preinstalled system rather than that the system must have to be downgraded in term of the performances.
- The access which is provided at the remotely basis should be controlled and monitored at equal time period.
- Whenever a new protocol is being designed it should have the ability for the incorporation of the security solutions which should be needed in the time of the future.

VI. PROPOSED SOLUTIONS

Smart Grid Security

The evolution of the power grid of the traditional nature is being done and it is converted into the smart automation grid. The integration of the modern power system automation grid of traditional nature is being done with the ICT (information and communications). By the help of these integrations the utilities of electricity are being controlled, monitored constantly, and is being managed as per the demand rate of the customers. Millions of the devices and millions of entities are combined together for the formation of the smart industrial automation grid system. Many malicious activities and the security issues are being gifted as with this type of enormous and massive network system [23].

The provision of the electricity is being done with the help of the distributed and centralized generation station and make sure that the customer should receive the undistributed and uninterrupted provision of the electric current, done by distribution and transmission systems. The grid is being used, monitored and controlled with the help of the ICT. The cost of the resource is decreased by this method and it is more efficient and reliable method for the delivery, moreover, the companies which are providing the technologies should have to put effort in the demand and control as these systems are already doing all the thing. By the help of the digital system of communication which is being generated in between the company and the customers, by the help of the information sent by the customer the smart grid has the capabilities to provide electric network which are based on the operation. The attacks are the most frequent fear for these type of companies as the smart grid network or system is very much vulnerable for these types of attacks. To prevent these attacks there are three main things which should be done [24]:

- The power should be supplied as per the requirement of the user.
- The communicated information should secure the integrity.
- The data provided by the user should be kept under strict confidentiality [24].

A) System Components

In the smart grid system, the major components are the energy resources which are renewable, the household appliances which are electrical in nature, the smart meter, the operation center which has the utilization of the electricity, and the provision of the services. All the devices which are being used in the home and which consumes energy are nowadays believes to have a smart and good communication system, known as the HAN (Home area network), and by the help of HAN the consumption of the power is being made very much effective and efficient related to all the devices used. The renewable resources involve the energy generated by the wind, energy generated by the sun which are used for the fulfillment of the energy need required by the home appliances and are known as the local electricity generator. The embedded system which usually tends to be alone is known as the smart meter. On each of the smart meter multiple facilities/features are may be present may not be present that are volatile or the non-volatile memory, digital/analog ports, clock of real time nature, timers, serial and clock communication facilities. The smart meters are said so for a reason that is, these are being equipped with the smart intelligent chips which are responsible for the control of the devices such as the air conditioner would turn off automatically if the room is reached on a specific temperature set. Smart meter can also be used in the management of the demand side of the system. The power consumption is also being minimized by the use of the smart meter [23].

B) Network Components

There are two communications which are being incorporated by the smart grid: WAN (wide area network) and HAN (home area network). By the help of HAN, the devices which are present in the house are being connected to the smart meter. The communication done by the HAN is done by the utilization of the wireless/wired Ethernet, Zigbee or the Bluetooth technology. On the other hand, the WAN is a network that is bigger in nature and it is utilized for the connection between different smart meters, electricity utilities and the service providers. The communication of the WAN could be done by the help of several technologies which includes the LTE/GSM/3G, fiber optics or the WiMAX. The smart meters are being used as the pathway by which the external parties and the in-house devices are being connected and the information of interest is passed on. The power utilization is being managed inside the smart grid system, collection of the hourly usage of power is also being measured by the smart meters, and if the attack is happening then the notification will also be sent to the smart grid. The HAN are only used in the homes where the residential lives, the IAN and the BAN are the one which are used in the offices and the industries respectively [23].

C) Vulnerabilities

Smart Grid familiarize the enhancements and enhances the capabilities to the conservative power network providing which are more complex and susceptible to various kind of attacks. By the help of these security issues the attackers are capable of many things such as the break of the confidentially, access to the network, the integrity of the data which is being transmitted hence it makes the service unavailable. Some of the most critical vulnerabilities are:

- *Security of the customers:* smart meters are originally collecting the huge amount of the data and the way for it to the utility company, the consumers and the service providers. The information includes isolated consumer info which is might be then used to conclude the devices being used, the consumer’s activities and the times whenever the home is vacant.
- *Immensely intelligent devices:* The smart grid has numbers of the intelligent devices which are in turn involved in the management of the network demand and the electricity supply. These intelligent devices are basically the medium of the entry in the network while the attack. Furthermore, the immensity of the smart grid creates the hindrance in the administration very difficult and the network monitoring.

- *Physical Security:* Not like the conventional power system, the smart grid networks comprise of numerous components and many of them are not included on the utility premises.

  These facts basically escalate the numbers of the self-doubting physical locations and hence the smart grid network becomes more vulnerable for the physical access.
- *The lifetime of the power systems:* it is noted that the power system is present with the comparatively short-lived IT system, it cannot be ignored that the equipment which are still in the service.

  These old and not trustworthy equipment is the security loophole which might be very well be mismatched with the present power systems and the devices.
- *Different Team's backgrounds:* incompetent and not the organized communication between teams may be the causing agent for the lot of the bad decisions and is being leading to the much susceptibility.
- *More stakeholders:* whenever there are numerous stakeholders the company or the system are under very critical kind of danger of the attack: the insider attack.

D) Attacks and their Types

There are multiple vulnerabilities which can be used by the attackers with multiple intentions and the competence and then the network could be damaged at a very large scale. The attacker may be of several types, such as, employees, elite hackers, script kiddies, customers, terrorists or the competitors.

Non-suspected attackers are the one who examine the security and the system of the operational system as the problem to solve. These attackers are being controlled by the curiosity and the intellectual challenges.

The customers are mostly having the intentions of the revenge and the cruelty as they show them against the other customers and then use the intellect for the shutting the power of the home.

The smart grid is the very keen target for the terrorists as if the smart grid is being hacked the destruction will be more visible. However, the employees may cause some of the errors which are mostly the unintentional errors.

Malware spreading: the virus could be developed by the attackers and then could be leaked to infect the company or the smart meters. This virus can manipulate the system to do some of the job which is not the work of the system by default such as the leaking of the sensitive information.

Access through the link of the database: for the record of the activities done on the system there are certain control systems which are present and these systems are made on the databases systems in which the network is further then mirrored as the logs of the business network. If the following management systems of the database are not securely and properly organized the business network database will become a very easy attack for the skilled attacker, and if the database is under the control of the attacker the system could be easily exploited.

Compromising communication equipment: the communication equipment for example the multiplexes could be compromised by the attacker which in turn be used in the causing of the damage or the compromised communication equipment can be used as the backdoor for the future attack initiator.

Relay Attack: false information could be injected in the network by the help of the packets sent by the attacker, for example, false prices, wrong meter data, the emergency events which are fake in nature etc. Electricity markets are at very greater risk on the financial state by the fake information.

Availability of the network: the smart grid basically uses the TCP/IP stack and the IP protocol, the susceptibility characteristics in the TCP/IP stack and it becomes a very keen subject for the DoS attack as well.

DoS attacks are done for the blocking, delaying or the corruption of the communications and it is done so that the resources of the smart grid are to become unavailable.

Traffic analysis and the Eavesdropping: An opponent of the company could be able to obtain the critical information by the help of the network traffic monitoring. The data could be of various types such as: the control structure used by the grid, information of the future price and the information of the usage of the power.

Security issues of the Modbus: the term mostly refer as the SCADA gives us the information used by the computer systems and their protocols which basically controls and monitors the facility-based processes and the infrastructure of the smart grid. As the smart grid was not basically designed for the high critical security issues, the attacks could be of several types:

- Fake messages could be sent to the devices which are basically known as the slave devices.
- The master receives the genuine recorded messages which are replayed by the attacker.
- One or the numerous field devices are controlled by the attacker as the master is locked out of the network.
- For the information derivations and the derivation of the addresses a benign message is sent to all the users.
- The messages of the Modbus are being read.
- The response messages are delayed which are basically intended for the master itself.
- The computer which have an appropriate adopter is being attacked.

VII. CONCLUSION & FUTURE WORK

The modern-day systems administration sphere has significance towards the operations of all industrial controller operations. From this approach ICPs convention principal has turned out to capable of a more trustworthy degree of satisfaction in control frameworks, security and plant monitoring prerequisites and is also generally executed for these characteristics. An extensive sort of blessings is offered by the industrial frameworks. These blessings include the recounted through their established order, less cost, low level field buses for appointing time, set up using the good field instruments and less demand of support. It also includes the high-level communication between logical controllers. This communication can be done by using the abnormal state field buses. It also includes the prominent joining of the inside controller frameworks with the outside systems. All in all, the advantages exceed the detriments and control arranges in some shape or frame is continually accomplishing a more noteworthy level of market infiltration.

The main focus of this research is to discuss the security challenges, threats and vulnerabilities of industrial communication protocols and then provide their possible solutions, as it is required for conventional industrial communication protocols towards the improved modern high-speed industrial communication Protocols (ICPs).

That is used for communications between the field devices and framework control application. Commercial networks are also known as domestically used networks like WIFI, LAN and telephone networks etc. To meet the modern industrial requirements, ICPs have to improve the standards used to determine how data transmission on communication network devices, Programmable logical controllers, Desktop PC's, and so on. The findings in the report are concluded with some security recommendations of the industrial communication system. In some systems the encryption is not implemented in most of the protocols of the industrial controls. Thus, it makes the system vulnerable as any unauthorized attacker can attack the system and check out that what are their traffic and also can manipulate the traffic by simply inspect their elements. There are some components which are making the infrastructure monitored periodically and should be followed up for the determination of patches and updates or there are also chances of detecting the defects or the emergence of the vulnerabilities. Some communication ways like peer to peer communication, deterministic communication and peer to peer communication.

There are some attack vectors an attacker will use to disturb the security of the industrial communications and these threat vectors are eavesdrop attack, DDOS attack, replay attack, brute force attack and dictionary attack. The attackers can violate the security of the system by doing these types of attacks. There are some ethernet and IP protocols based on the ethernet which use the IGMP and UDP. It is suggested to undertake the passive monitoring of the network to ensure the traffic of the ethernet and IP is associated with the pieces of the equipment and it doesn't come from the outside network. Focusing on the security issues mentioned in the report the communication has to be controlled properly in the MODBUS. There is a need to make some checks on the MODBUS TCP packets for the error data about the size and traffic through the TCP port 502 will incorrectly form packages. There are total eight security objective that must be fulfilled properly for the better security of the industrial control system these objectives are secretiveness,

probity, accessible, authentication of users, User authorization, exploration, non-reputability and third-party security protection. Modern industrial control systems required better and improve industrial communication protocols. To resolve the issues and address security threats and vulnerabilities of industrial communication protocols (ICP's), we will propose a security framework which will be capable to fulfil the requirements for the modern Industrial Communication Networks/Systems. The proposed framework for Industrial Communication Protocols will consist of the following components (Fig. 1).

- Secure Transmission Method
- Improved architecture of Industrial Communication Network
- Physical characteristic
- Secure Real-Time/Historical Plant Parameters Data Monitoring
- Better GUI Libraries
- Diagnostic Features

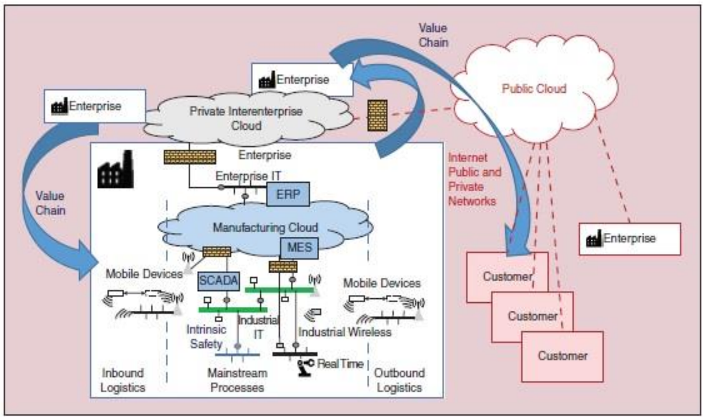

Fig. 1: framework for Industrial Communication Protocols

REFERENCES

[1] T. Sauter, S. Soucek, W. Kastner, and D. Diet-rich, "The evolution of factory and building automation", IEEE Ind. Electron. Mag., Vol. 5, No. 3, pp. 35–48, March 2011.

[2] M. Guarnieri, "The roots of automation before Mechatronics", IEEE Ind. Electron. Mag., Vol. 4, No. 2, pp. 42–43, June 2010.

[3] G. Fettweis, H. Boche, T. Wiegand, E. Zielinski, "The tactile Internet", International Telecommunication Union. Geneva, Switzerland, August 2014.

[4] A. W. Colombo, S. Karnouskos, Y. Shi, S. Yin, and O. Kaynak, "Industrial cyber–physical systems: scanning the issues", Proc. IEEE, Vol. 104, No. 5, pp. 899–903, May 2016.

[5] A. J. C. Trappey, C. V. Trappey, U. H. Govindarajan, J. J. Sun, and A. C. Chuang, "A review of technology standards and patent portfolios for enabling cyber-physical systems in advanced manufacturing", IEEE Access, Vol. 4, pp. 7356–7382, October 2016.

[6] R. Venkatesan, M. V. Raghavan, and K. S. Sai Prakash, "Architectural considerations for a centralized global IoT platform", in Proc. IEEE Region 10-Symp., pp. 5–8, May 2015.

[7] WANG Shan, WANG Hui-Ju, QIN Xiong-Pai, ZHOU Xuan. Architecting Big Data: Challenges, Studies and Forecasts, Chinese Journal of Computer. 2011, 34(10): 1741-1752.

[8] Flower. et al et al., "Incident-based matrix Provide an integrated approach to viewing cyber incidents. vol. 4, pp. 51-79, 2019.

[9] Flower. et al et al., "Cyber attacker taxonomy "Increase awareness of categories of attackers in ICS cyber incidents, can be used to complement other taxonomies.2018, p. 178.

[10] Oltramari et. al., "Ontological approaches to SCADA vulnerabilities or attacks" 2016, pp. 689-694.

[11] Smith. et al., "A Proposed taxonomy for vulnerabilities", vol. 23, pp. 767-782, 2016.

[12] Line. et al., "Taxonomy of cyber-attack on SCADA System, IEEE Transactions on Industrial Electronics, Vol. 57, No. 11, pp. 3614–3621, Nov 2015.

[13] Zhu. et al., “A taxonomy of targeted attacks”, In 2014 22nd IEEE International Symposium on Computer-Based Medical Systems (pp. 1-5), 2014.

[14] Fleury. et al., "Attack-vulnerability-damage model” in 2013 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), vol. 17, pp. 501-507, 2013.

[15] J. Kjellsson, A. E. Vallestad, R. Steigmann, and D. Dzung, “Integration of a wireless I/O interface for PROFIBUS and PROFINET for factory automation”, IEEE Transactions on Industrial Electronics, Vol. 56, No. 10, pp. 4279–4287, October 2009.

[16] J.P. Thomesse, “Fieldbus technology in industrial automation”, Proceedings of the IEEE, Vol. 93, No. 6, pp. 1073–1101, June 2005.

[17] R. Lagner, “Cracking stuxnet - a 21stcentury cyber weapon”, http://www. ted.com/talks/Ralph-langner-cracking-stuxnet-a-21stcenturycyberweapon.html, [Accessed on April 2017].

[18] Matrosov, E. Rodionov, D. Harley, and J. Malcho, “Stuxnet under the microscope”, ESET, Tech. Rep., 2014.

[19] Novak and A. Gerstinger, “Safety and security-critical services in building automation and control systems”, IEEE Transactions on Industrial Electronics, Vol. 57, No. 11, pp. 3614–3621, November 2016.

[20] T. Sauter, “The three generations of field-level networks – evolutionand compatibility issues”, IEEE Transactions on Industrial Electronics, Vol. 57, No. 11, pp. 3585–3595, November 2017.

[21] Khalid Imtiaz, Ali Abid Abidi and M. Junaid Arshad “Comparative Analysis of Industrial Control Communication Network Protocols’’ International Journal of Computer Science and Telecommunications [ISSN 2047-3338], Vol. 8, Issue 1, January 2017.

[22] Miguel Herrero Collantes, Antonio López Padilla Protocols and Network Security in ICS Infrastructures

[23] Aloul, F., Al-Ali, A.R., Al-Dalky, R., Al-Mardini, M. and El-Hajj, W., 2012. Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy, 1(1), pp.1-6.

[24] Al-Omar, Ban, A. R. Al-Ali, Rana Ahmed, and Taha Landolsi. "Role of information and communication technologies in the smart grid." Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 5 (2012), pp: 707-716.

[25] Wei, Dong, Yan Lu, Mohsen Jafari, Paul Skare, and Kenneth Rohde. "An integrated security system of protecting smart grid against cyber-attacks." In 2010 Innovative Smart Grid Technologies (ISGT), pp. 1-7. IEEE, 2010.

[26] Dzung, Dacfey, Martin Naedele, Thomas P. Von Hoff, and Mario Crevatin. "Security for industrial communication systems." Proceedings of the IEEE 93, no. 6 (2005): 1152-1177.

[27] E. Cole, Hackers Beware. Indianapolis, IN: New Riders, 2002.

[28] Drias, Zakarya, Ahmed Serhrouchni, and Olivier Vogel. "Analysis of cyber security for industrial control systems." In 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), pp. 1-8. IEEE, 2015.

[29] Al-Hamdani, Wasim A. "Missing factors in teaching cryptography algorithms for information security tracks." In 2009 Information Security Curriculum Development Conference, pp. 15-20. ACM, 2009.

[30] IEEE-USA. (2000) Position: Information security in electric power, part of the IEEE-USA legislative agenda for the 107th Congress.

[31] Chi, Qingping, Hairong Yan, Chuan Zhang, Zhibo Pang, and Li Da Xu. "A reconfigurable smart sensor interface for industrial WSN in IoT environment." IEEE transactions on industrial informatics 10, no. 2 (2014): 1417-1425.

[32] Jaloudi, Samer. "Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study." Future Internet 11, no. 3 (2019): 66.Albert-Lszl Barabsi. The network takeover. Nature Physics, 2012, 8(1): 14-16.

Khalid Imtiaz is an Engineer, Computer Science researcher and Team Leader (Automation of the Industrial Process Solution), Lahore-Pakistan from year 2014 till now. He received his B.Sc. Electrical (Computer) degree from Comsats-Lahore in year 2014, and an M.S (CS) degree from UET-LHR in year 2018. His research interests span both computer networking and data science. Much of his work has been on improving the understanding, design Industrial Networks Protocols.