❏   1359

Augmentation of a SCADA based firewall against foreign hacking devices

Abhishek Mungekar[1], Yashraj Solanki[2], R. Swarnalatha[3]

[1,2]Department of Electronics and Instrumentation Engineering, Birla Institute of Technology and Science, Pilani
Dubai Campus, Academic City, Dubai, United Arab Emirates
[3]Department of Electrical and Electronics Engineering, Birla Institute of Technology and Science, Pilani,
Dubai Campus, Academic City, Dubai, United Arab Emirates

Article Info	ABSTRACT
	An Industrial firewall is a system used to supervise and regulate traffic to and from a network for the purpose of securing appliances on a network. It analyzes the data passing through it to an already defined surveillance criteria or protocols, discarding data that does not meet the protocol's requirements. In effect, it is a filter preventing undesirable network traffic and selectively limiting the type of transmission that occurs between a secured transmission line. In this research paper a SCADA based Firewall is implemented for protection of the data transmission to a PLC, against external hacking devices. This firewall is virtually exposed to several external hackers and the degree of vulnerability is carefully studied, in order to develop an ideal Firewall.

Corresponding Author:

R Swarnalatha,
Department of Electrical and Electronics Engineering,
Birla Institute of Technology and Science, Pilani Dubai Campus
Dubai International Academic City, Dubai, United Arab Emirates.
Email: swarnalatha@dubai.bits-pilani.ac.in

1. INTRODUCTION

In the year 2000, an unnamed sewage control system in Queensland, Australia, faced several difficulties from the moment it was installed by the manufacturer. Most of these problems continued for several of the following months; with pumps not responding and running when required to, a complete loss of transmission between the control room and the pumping stations etc. These lead to several months of flooding in several of the nearby communities and a river with several tons of sewage.

An insight into several of the industrial cyber-attacks is that they are very difficult to identify, this case was no different. The attacker linked with this attack managed to attack the system a total of 46 times, until the unknown entity was caught. At the onset it was considered that a leakage in the pipes must have been the root cause of all the problems. Only after months of data logging it was discovered that several of the controllers were hacked, and would activate the valves randomly without a command being initiated at the remote control rooms. Later it was discovered that, one of the ex-employee of the contractor company was behind all these hacking attempts in order to be hired by the company to resolve these issues [1]. The above case study is an indicator on why protecting these industrial control systems is crucial. Development of highly sophisticated industrial firewalls can prevent such a haphazard [2, 3].

In these recent times, Industrial control systems have increased their dependence on several typical internet protocols such as Ethernet, TCP/IP and Windows for transmission of sensitive or non-sensitive information. Utilization of these protocols in large scale industrial systems have become a lot more networked and easily reachable from any portion of the world, making them a lot more vulnerable to a cyber

threat. Moreover, the rising reliance over internet-connected devices, also known as Internet of things is making the devices more susceptible to Cyber-attacks.

Keeping all the above risks in mind, when Supervisory control and data acquisition engineers or experts are questioned over the actual threats to industrial control systems, often cast a blind eye over the entire issue by claiming that specially designed communication protocols and exclusive automation systems would incorporate to all the external factors affecting the systems [4-7]. The proposed ideology, suggests a SCADA based Firewall which is implemented for shielding the data transmission to a PLC, against extrinsic hacking gizmos. This firewall is virtually exposed to extrinsic hackers trying to override TCP interface protocols and further improvisations are incorporated based on the pattern observed in order to develop a germane firewall.

2. GENERALIZED OVERVIEW ON FIREWALLS

Firewalls are crucial accessories in the field of cybersecurity, for protection of several industrial based PC's, control systems or as in the above case a large scale Industrial sewage systems.

2.1. Importance of firewalls

A wide range of firewalls persist in today's market, with unique attributes associated with each one of them. The two major categories of distinction are Host firewalls and Networked Firewalls. The Host firewalls are installed on Personal Computers or in several operating systems, which are mainly software based. These windows operating based firewalls installed in almost every computer or PC are these days to protect them from malicious attacks over the internet [8-10].

The later type of firewall is called a networked firewall and as the name suggests, is the type of firewall which part of a networked system unlike the host based firewall. Figure1 is a depiction of such type of industrial networked firewalls. These types of networks can usually be found in large scale industries, which store data on a centralized server, which can easily be accessed by several authorized professionals based on access codes. These Distinctive firewalls are utilized in various sites within a networked system to provide different types of security as part of a strategy. They help in safeguarding the link between company's network and the industrial network, by securing them against hackers. Likewise, several types of firewalls are devised with specific set of rules, to limit a specific type of communication. The concept of decisively limiting communication between members within the network, as well as separating of various network areas from each other, is known as Zones and Conduits [11].
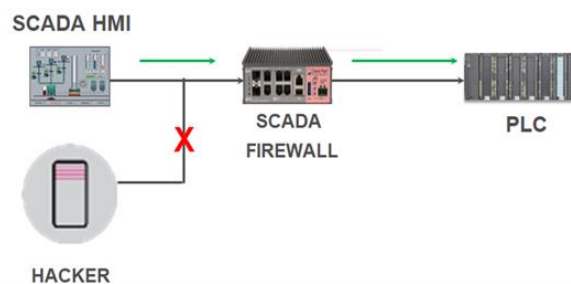

Figure 1. Generalized Industrial Firewall working diagram

2.2. The differences between IT and industrial firewalls
2.2.1. Security priority

The first and foremost difference between the Industrial and I.T firewalls is in terms of security priority. In the case of Industrial Control System (ICS), focus is shifted to the availability, visibility in various processes and the operations involved, integrity and at last the confidentiality aspect. On the other hand, IT has kept its first priority on confidentiality followed by integrity and at the end towards availability [12].

2.2.2. Service providing and latency

In terms of latency ICS is always based on the real-time requirements which is of a vantage point as for IT the response times tend to be varying in nature. ICS is functional 24 hours by 7 days by 365 days per year whereas as IT needs to be restarted when it is needed to do so.

2.2.3. Software robustness

For ICS, apart from the case of a benign environment protocols tend to fail only when challenged. For IT, there are implementations which are put under continuous hacker scrutiny and then the weaknesses are eliminated.

2.2.4. Technical and economic span

One key difference between ICS and IT is the technical and economic lifespan. The periods typically used for 'writing-off' ICS are very long when compared to the periods in which organizations 'write off' IT. Typical ICS therefore have an installed base of aging technology, the so-called legacy ICS, which often includes supplier-specific applications and hardware, and decades-old communication protocols and hardware [13].
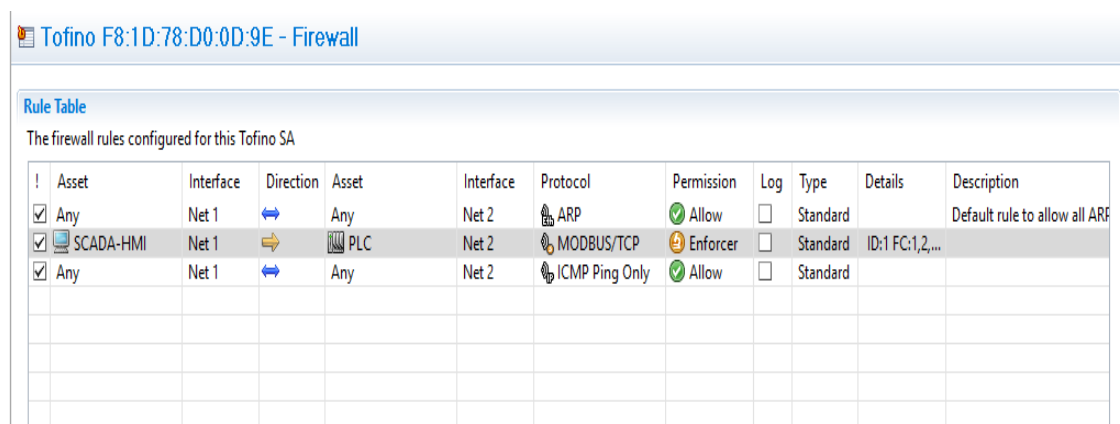
2.2.5. Depreciation

ICS records about 10 to 25 years of the depreciation value whereas IT only records 3 to 5 years which far less in comparison to the ICS.

2.2.6. Safety instrumented systems

Plant safety is a crucial part of plant operation, and ICS. Therefore, the ICS often include integrated, yet distinctive, safety instrumented systems (SISs). The SIS is responsible for ensuring and maintaining the safe operations of the process by placing the process into a safe state when process conditions that threaten safety are detected. IT systems have no systems analogous to the SIS [14-15].

3. INDUSTRIAL FIREWALL CONFIGURATION

Tofino is a modernized Industrial Control System firewall, which unlike it's I.T firewall counterparts also accepts SCADA protocols. This particular project involves utilization of two user-defined assets as suggested in Figure 2. SCADA-HMI and PLC are the two defined assets. These assets function on the basis of two primaries and one secondary protocol. The two primary protocols are mandatory for the software, while the secondary protocols can be defined to enable several other form of communication as per user requirement.

Tofino F8:1D:78:D0:0D:9E - Firewall

Rule Table

The firewall rules configured for this Tofino SA

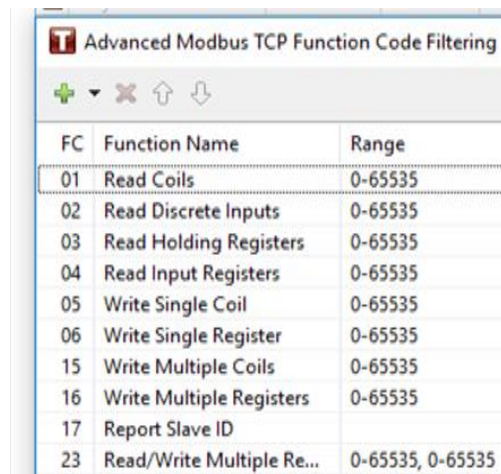| !	Asset	Interface	Direction	Asset	Interface	Protocol	Permission	Log	Type	Details	Description
☑	Any	Net 1	⬌	Any	Net 2	ARP	Allow	☐	Standard		Default rule to allow all ARP
☑	SCADA-HMI	Net 1	⬌	PLC	Net 2	MODBUS/TCP	Enforcer	☐	Standard	ID:1 FC:1,2,...	
☑	Any	Net 1	⬌	Any	Net 2	ICMP Ping Only	Allow	☐	Standard		

Figure 2. User-defined asset designation

3.1. Address resolution protocol

The First and foremost protocol being the Address resolution protocol (ARP), which is set by default by the firewall in order to recognize the Mac Address, associated with a given internet layer address, like an IPv4 address as utilized in this case, which is important for the functioning of internet protocol suite. This is a distinctively better form of encoding as compared to considering only an IP address of the device. This mapping process reduces vulnerability towards hacking by a significant margin. It is vital to keep the flow of data bi-directional for any given asset.

3.2. Transfer control Protocol

The second primary protocol is the MODBUS/TCP protocol.This is responsible for transmission of data from one user to other, by defining distinct set of rules. The permitted communication lines for this protocol are enforced. This means that only uni-directional flow of data is permitted along with this protocol. The permission is enforced from the SCADA-HMI to the PLC. This is developed on the basis of certain types of function codes as suggested in Figure 3, these function codes enable the firewall to read and write coils, discrete inputs, holding and input register in addition reporting the Slave ID. While defining the assets for the SCADA-HMI and the PLC in the above protocol, it is critical to define their respective MAC and IP addresses.
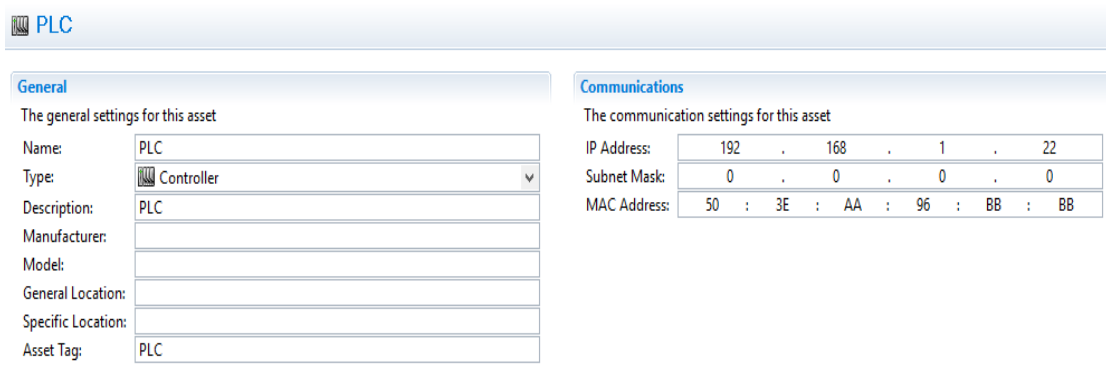

Figure 3. Function codes set-up

4.   MASTER AND SLAVE SIMULATOR CONFIGURATIONS

A typical master and slave ideology is implemented in this section, where information generated at the slave end of the system will be extracted by the master.

4.1. Modbus simulator (slave)

This particular simulator as suggested in Figure 4 will virtually represent the Programmable Logic Controller. The PLC will mimic as a slave to the SCADA HMI. ModSim64 connection includes connecting to the Modbus/TCP server. The following window includes the address of the offset provided, Length of the array, Device id and the type of MODBUS point type introduced. Different point types can be assigned based on the user-requirement; these include Holding registers, Input registers, Coil status and Input status. For the intent of this project, Input Registers have been considered.

Figure 4. Modbus PLC simulator configuration

4.2. Interactive graphical SCADA system (IGSS)

Interactive Graphical SCADA system is an automation based software developed by Schneider electric. In the following sections, the software has been utilized to develop the human user interface for accessing data from the PLC simulator [16].

4.2.1. SCADA-HMI (master)

The system configuration of this software, involves setting up a remote and local IP. This is followed by selecting the protocol over which the transmission of data occurs. The protocol used is MODBUS/TCP. The offset is defined here, such that it points to the position of the data acquired from the slave. After the HMI is configured, the design mode is selected for defining tag name, type and attributes. Once the tag is defined, the simulation is ready to use [17]

This project utilizes a flow defined parameter, which can be created by using the definition function in the IGSS software. The area properties employed in this section consist of defining a default driver, suitable for the communication between the Slave and the master. The default driver used is a Demo-station for 7TMODTCP.The flow defined object creation takes place with respect to object type. The object type defined is analog. This is followed by selection of symbols under the Symbol definition table. Implementing the enable option, allows the user to supervise the value or state of the flow.

The subsequent atom mapping category will handle the atom properties and the slave offset address Enabling. The actual value option proves to be very decisive, as it ensures the original data is captured from the Slave [18-20]. The slave offset address includes defining the data type as Read input registers. This is done in-order to co-relate with the slave. The corresponding offset defined in decimal and hexadecimal, will point out the value from the Slave simulator. Since the values are being extracted from the slave as an input for the master, hence the I/O mode opted will be of input type. The settings defined in the atom mapping section will be reflected in the analog segment of the object properties [21]. Once the settings are imminently carried out, the individual I.P and MAC addresses are updated as indicated in Figure 5, to establish the Master simulator on the same network as the PLC simulator.

Figure 5. SCADA-HMI Configuration on the firewall

4.2.2. SCADA-HMI (attacker)

The setup for the attacker will remain the same as the master along with distinct IP address. The device Unit Id and port number for both the SCADA-HMI (Attacker and Master) and Modsim64 simulator should always remain the same. Figure 6 is the display utilized to supervise the data flow in the master and as well as the attacker.

5. PROPOSED METHODOLOGY AND PERFORMANCE EVALUATION
5.1. Without firewall scenario

After setting up the Slave, Master and the Attacker they all need to be configured to a particular range of IP. Before commencing the scenario, test the ping between all the three systems respectively. This ensures a stable communication between the systems and connecting switch involved. An offset declared in IGSS will be extracted from Modbus simulator. This data extracted will be transmitted to the Master and Attacker SCADA-HMI. The dual transmission of data occurs due to absence of a firewall.

Hence, allowing the attacker access to the Modbus simulator. The offset set in the PLC configuration is originally, 55. Due to the absence of the firewall in this scenario, the original reading is transferred to the interface, which makes it easier for the hacker to conceive information from. Figure 6 displays the hacker's screen, being able to obtain the offset change in the PLC [22].
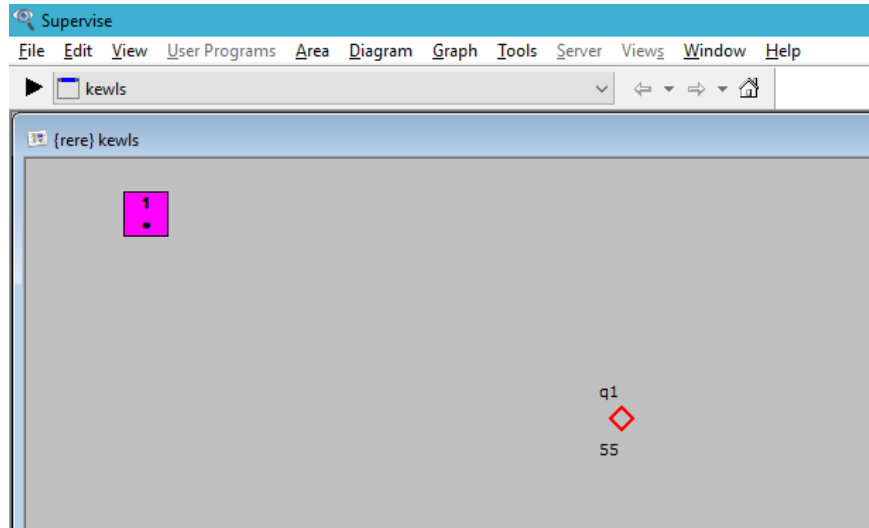

Figure 6. Hacker SCADA-HMI (without firewall)

5.2. With firewall scenario

In this scenario a firewall is introduced between the Master and the slave as shown in Figure 7. The Net 1 port of the firewall is connected to the Master SCADA-HMI, while the Net 2 port is connected to the slave PLC simulator. The remaining connection stays the same as the without firewall scenario. The Firewall is ready to use, due to the previously defined assets. The use of this firewall prevents the attacker from accessing the PLC simulator on the basis of a standard protocol. From the figure, due to the presence of the firewall, is selectively ruling out the hacker. Thereby, obscuring the original offset change from the PLC.
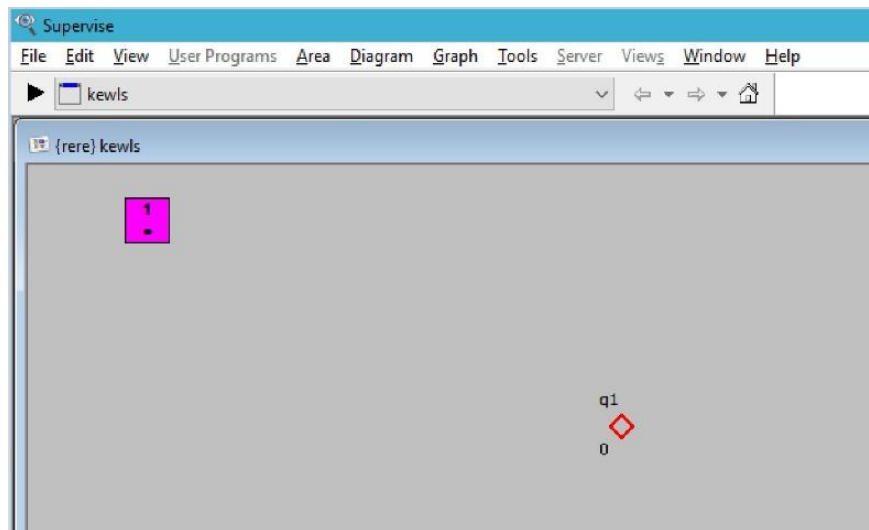

Figure 7. Hacker SCADA-HMI (with firewall)

6.   RESULTS AND CONCLUSION

This paper provides a generalized insight on the requirement of firewalls in the case of Industrial control systems. The major surveillance criteria's have been addressed, followed by providing a stark contrast been an IT and an Industrial firewall. The above proposed idea could certainly prove useful in major industrial units. A major point that should be taken into consideration is that, there is no such customized firewall present in the market to tailor all the security protocols. Moreover, as cyber-attacks get more and more fatal, regularly updating these pre-defined protocols is crucial [23]. The idea proposed above is one out of many, in the field of Cybersecurity of control systems. At the moment encoding with the help of MAC and I.P addresses is a very unique way of tackling external traffic within the network. More sophisticated methods of encoding can be developed to assure even higher level of security [24, 25]. Working scenario with all three devices connected to one single network as shown in Figure 8.
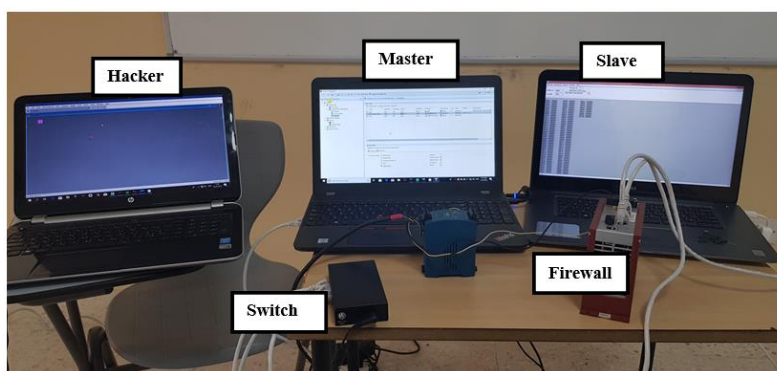

Figure 8. Working scenario, with all three devices connected to one single network

REFERENCES

[1]   Cardenas, A. A., Amin, S., And Sastry, S.,"Secure control: Towards survivable cyber-physical systems", In *Proceedings of the First International Workshop on Cyber-Physical Systems*. (June 2008).

[2]   Cheung, S., Dutertre, B., Fong, M., Lindquist, U., Skinner, K., and Valdes, A. "Using model-based intrusion detection for SCADA networks", *In Proceedings of the SCADA Security Scientific Symposium* (Miami Beach, FL, USA, 2007.

[3]   Gao, "Information security, TVA needs to address weaknesses in control systems and networks", *Tech. Rep. GAO-08-526, Report to Congressional Requesters*, May 2008.

[4]   Marschall Abrams and Joe Weiss, "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia", Boston.

[5]   John H. Marbuger, I., and Kvamme, E. F, "Leadership under challenge: Information technology R&D in a competitive world. An assessment of the federal networking and information technology R&D program." *Tech. rep., President's Council of Advisors on Science and Technology*, August 2007.

[6]   Stouffer, K., Falco, J., and Kent, K, "Guide to supervisory control and data acquisition (scada) and industrial control systems security". *Sp800-82, NIST*, September 2006.

[7]   US-CERT, "Control Systems Security Program. US Department of Homeland Security", http://www.uscert.gov/control systems/index.html, 2008.

[8]   Luiijf, H.A.M., "Process Control Security in the Cybercrime Information Exchange", *NICC, The Hague*, the Netherlands, 2010.

[9]   NCSC, "Checklist Security of ICS/SCADA systems", factsheet 2012-02, Ministry of Security and Justice, The Hague, The Netherlands, 2012.

[10]   MSB, "Guide to increased security in industrial information and control systems", *Swedish Civil Contingencies Agency*, Stockholm, Sweden, 2014.

[11]   M. Oosterink, "Security of legacy process control systems: moving towards secure process control systems" (whitepaper), The Hague, The Netherlands, 2012.

[12]   Hurd, S., Smith, R., AND Leischner, G. "Tutorial: Security in electric utility Control systems". In *61st Annual Conference for Protective Relay Engineers (April 2008)*, pp. 304–309, 2008.

[13]   Stewart A.Boyer, " SCADA: Supervisory Control and Data Acquisition", *International Society of Automation* 2009.

[14]   Gregory K. McMillan, "Process/Industrial Instruments and controls Handbook" McGrAW-HIL 1999.

[15]   J. Viega and M. Messier, "Security is harder than you think," *ACM Queue*, vol. 2, pp. 60–65, Jul/Aug. 2004.

[16]   Tidrea, Alexandra & Korodi, Adrian. (2018). WebNavIGSS Web-Based Software Solution for IGSS SCADA Applications. 418-423. 10.1109/MED.2018.8442560

[17]   Keith Stoufler, Susan Lightman, Marshal Abrams, "Guide to industrial control systems Security", *NIST special publication,* pp. 800–82, May 2014.

[18] K. McMillan Gregory, "Process/Industrial Instruments and controls Handbook" in , McGrAW-HIL, 1999.
[19] Paul Didier, "Reference Architectures for Industrial Automation and Control Systems", *ODVA Industry Conference & 15th Annual Meeting*, October 2012.
[20] M.J. Karam, F.A. Tobagi, "Analysis of the delay and jitter of voice traffic over the Internet in", *Proc. of IEEE INFOCOM '01*, 2001.
[21] P. Neumann, "Communication in industrial automation - what is going on" in *Control Engineering Practice*, Elsevier Ltd, vol. 15, pp. 1332-1347, 2006.
[22] D. Dzung, M. Naedele, Hoff T.P. Von, M. Crevatin, "Security for Industrial Communication Systems", *Proceedings of The IEEE*, vol. 93, no. 6, JUNE 2005.
[23] Standards for Security Categorization of Federal Information and Information Systems National Institute for Standards and Technology FIPS 199, February 2004.
[24] "Minimum Security Requirements for Federal Information and Information Systems National Institute for Standards and Technology FIPS 200", Framework for Improving Critical Infrastructure Cybersecurity. NIST February 2014, March 2006.
[25] M. B. Line, I. A. Tondel, M. G. Jaatun, "Cyber security challenges in Smart Grids", *Innovative Smart Grid Technologies (ISGT Europe) 2011 2nd IEEE PES International Conference and Exhibition on*, pp. 1-8, 2011.

BIOGRAPHIES OF AUTHORS

Abhishek Anil Mungekar is currently pursuing Bachelor of Engineering with Honors in Electronics and Instrumentation Engineering in Bits Pilani Dubai Campus. His area of interest is Cybersecurity, Systems Control & Instrumentation

Yashraj Kalpesh Solanki is currently pursuing Bachelor of Engineering with Honors in Electronics and Instrumentation Engineering in Bits Pilani Dubai Campus. His area of interest is Cybersecurity, Automation & Instrumentation.

Dr. R. Swarnalatha did her BE in Instrumentation & Control Engineering from Sathayabama Engineering College, Chennai and M.E in Instrumentation Engineering from Madras Institute of Technology, Anna University, Chennai. She received her PhD degree in Biomedical Instrumentation from Birla Institute of Technology and Science (BITS), Pilani, India. She has 20 years of teaching experience. She is working with BITS Pilani, Dubai Campus for past 14 years. She has guided many projects and taught various courses for undergraduate and postgraduate students. Her research interest includes biomedical instrumentation, process control & Instrumentation, neural network & fuzzy logic.