Modern SCADA Systems

A review on Modern SCADA Systems and Security Considerations of Individual SCADA system component

[1]Neel H. Pathak, [2]Prof. H. B. Patel

[1]M.E. Research Student, [2]Head of Department (L.C.I.T.)
I.T. Systems and Network Security, Computer Engineering Department
Gujarat Technological University PG School, Ahmedabad, India
[1] neel.pathak@yahoo.com, [2]hasmukh.patel@lcit.org

***Abstract* - Supervisory Control and Data Acquisition (SCADA) systems, a part of Industrial Control Systems (ICS) are widely used for automation and control in many industry sectors like chemical plants, electric power grids, oil and gas plants etc. Traditionally these (i.e. SCADA) systems were operated in standalone manner, typically housed within the industries, chemical plants and other such electrical and mechanical industries. However, due to the expansion of business and the need to centrally monitor and control these systems, they are now being connected to a completely alien world, the world of Internet. As these systems are now being interweaved forming a small network similar to LAN and connected to the internet, they are prone to plethora of attacks prevailing not only on internet but also within the SCADA network. One can imagine the consequences if these critical systems are tempered or illegally taken control off. We must know that when SCADA systems are compromised then the loss would not just be financial and/or business function but also THE LOSS OF LIFE. In this paper, we first discuss about the modern SCADA systems, how they operate along with its problem description, how they are different from other Business/I.T. systems and/or networks. We also explain the famous CIA triad of Information Security from SCADA system`s perspective. Finally, we will shed light on the security of individual components operating within SCADA network by, categorizing components as physical and logical.**

***Index terms* - Modern SCADA Systems, SCADA, SCADA Security, C-I-A triad, Cyber-attacks, Component security.**

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are one of the most discussed systems today regarding its security among other Business/I.T. systems. So, it becomes necessary for us to first understand these systems and how they actually operates. SCADA systems are considered as one of the types among various Industrial Control Systems (ICS). These systems refer to the combination of telemetry (i.e. communication) and data acquisition [1]. Such systems have been constantly evolved, time to time. If we talk about the context of their evolution then they can be divided into following 3 generations [2], [3].

1. **First Generation or Monolithic SCADA systems:** These SCADA systems refer to those where no connection between them exists. These systems used to operate in a stand-alone manner.
2. **Second Generation or Distributed SCADA systems:** Such systems used to be connected and were more confined within small areas like LAN. These systems employed distributed architecture where there may be multiple clients or stations.
3. **Third Generation or Networked SCADA Systems:** These are those SCADA systems that makes use of networks and internet extensively. This is due to the standardization of network and wide use of internet. This is what we refer as modern SCADA systems.

According to [4], a new type of SCADA System has recently emerged called as "Fourth Generation SCADA systems or Internet of the things systems". Such systems use cloud computing as their base and adopt "Internet of things"[5] technology to reduce infrastructure costs and increase ease of maintenance and integration.

One should remember that Distributed Control Systems (DCS) are not actually SCADA systems [1]. DCS`s are employed within more restricted or confined area and usually forms a closed loop for their operation. On the other hand SCADA systems have no such confined network boundaries and covers large geographical areas.

Every coin has two faces, connecting SCADA network with internet helped many SCADA personnel and operators to operate from geographically distant location but this facility has also introduced problems related to SCADA system and network security. SCADA systems that are categorized as Third Generation and Fourth Generation is what we refer as modern SCADA systems.

As these systems are considered as any nation`s critical infrastructure system they are of prime target to Cyber Terrorists, Hackers and State sponsored attacks done through some cyber security professional.

Overview of Modern SCADA systems

Modern SCADA systems follows Master/Slave (or Client/Server) architecture model. As mentioned above it comprises of telemetry and data acquisition. Telemetry is used for communication between client and server (i.e. for transmitting and receiving data or information) over some specific medium. Medium such as cable, telephone or radio links is extensively used and the information/data to be communicated can be measurements like speed, flow or voltage.

The communication within SCADA systems (i.e. between Client and Server) can be of two types [1], first is Polled Mechanism. In such mechanism within a specific interval of time the master makes regular polling of data to each slave in sequence. The slave unit reacts to the master`s requests only when slave receives request from master. Second type is Interrupt System, such systems are so configured that when slaves reaches a certain measurement limit or notice a significant change in its input then it raises an exception and an event is triggered which transmits exception information to master. So, basically here the slaves initiate the communication with master. Notice that a SCADA system may have one master and many slaves or it may be vice versa.

Data Acquisition as the name suggests is a method to capture the data/information from equipment being monitored and controlled. Data/Information so captured can either be in an analog form or digital form. The state of any systems is best represented with digital form ON/OFF or 1/0 and those system whose information varies in a range (for example regulator) is represented in analog form. Now let`s identify the major components that are used for the operation of SCADA system. SCADA system is actually composed of many components, the major are:

1. ***Central Monitoring Station* (CMS):** The CMS actually refers to the location of master host station and is responsible for issuing commands to slave's machine through communication network. It also receives commands from slaves and either process them or store them for future reference.
2. ***Man Machine Interface* (MMI):** MMI or Human Machine Interface (HMI) is the interface that directly interacts with the operator/personnel of SCADA system for giving commands from CMS to remote stations and receiving commands from remote stations.
3. ***Programmable Logic Controller (PLC) and Remote Terminal Unit (RTU):*** At remote stations PLC`s and/or RTU`s are used. PLC`s are considered as miniature industrial computers which are used to replace relay logic of a plant or process. RTU`s are more ruggedized computers with very good radio interfacing. It is majorly used where communications are more difficult to establish.
4. ***Sensors and Actuators:*** These are small components that are directly interfaced to the industrial electrical or mechanical plant. The PLC and/or RTU`s receives the signals, process it and forward to these components. These components in turn does the actual work.
5. ***Transmission Media:*** Transmission Media is used for transferring information/data to the remote site and receive the same from remote site for decision making purpose. The media used can be either wired or wireless. Now a day's wireless media is more encouraged as it helps to connect geographically distant locations to connect with ease.

SCADA protocols especially Modbus [6] and DNP3 [7] plays a major role in the operation of SCADA systems. As modern SCADA systems are networked, their communicating behavior is dependent on the type of the protocol used for the communication between Masters and slaves. Now we have acquired knowledge about modern SCADA systems and how they work, the remainder of this paper is organized as follows. Section 2 discusses the problems related with SCADA systems. Section 3 mentions the related work done to mitigate the problems related to SCADA systems. Section 4 distinguishes the SCADA systems from traditional Business/I.T. systems and explains the famous C-I-A triad of Information Security from SCADA security perspective. In section 5 we identify and consider some of the SCADA components categorized as physical & logical and also discuss the ways to secure these components.

II. PROBLEMS RELATED WITH SCADA SYSTEMS

We have classified the problems related to SCADA systems and network in two broad categories. First is Technical Problems which deals with the technicalities of SCADA systems and second is Non-Technical Problems which will deal with non-technical aspects of the same. Although, such differentiation is only for grouping purpose. Let`s start with Non-Technical Problems first.

Non-Technical Problems

In [8] author mentions many non-technical problems related to SCADA network and SCADA Systems such as Insider Threat, Open unbounded and interconnected networks, Lack of firm security policy, Lack of regular audits of SCADA system etc.

Standards plays important role in interconnectivity with other systems and networks, it helps to audit the SCADA systems and also helps vendors in manufacturing systems but, due to lack of accurate standards of SCADA systems these objectives are not attained. If we look at Bureau of Indian Standards (BIS) [9] then also we can`t find any proper standards for SCADA systems.

As mentioned earlier physical access control to such systems should be taken care off. No one else except the operators/personnel of SCADA system shall have physical access to such systems. We have noticed many such places where there is no such physical access protection to such systems. Now let`s discuss the other part of problems i.e. Technical Problems related to SCADA systems.

Technical Problems

Unlike Non-Technical problem which deals with policies, procedures, standards and control access, technical problems deals with all the technicalities related to SCADA network may it be SCADA systems, SCADA Protocols or transmission media. Representing all the technical problems in a single paper is actually not possible so, we highlight only major of them.

Problems related with SCADA protocols

Most of SCADA protocols were designed a long before the era of network security [10]. Protocols like Modbus and DNP3 are mostly used for communication between HMI and PLC (or MTU`s and RTU`s). In fact most of SCADA protocols were designed not keeping security in mind. If we consider Security, Ease of Use and Functionality triangle [11], SCADA system were designed for ease of use and functionality as a result it lacks security aspect within these systems. In [12] author mentions the complete taxonomy of attacks on DNP3 protocol.

In short majority of legacy SCADA protocols don`t provide the following functions:

1. Authentication, any Node can claim to be a master and send control signal to slaves.
2. Confidentiality, anyone with little inclination can intercept SCADA traffic and learn its internal details along with its control messages as they are in plain text.
3. Integrity, there is no way one can say that the control signal is not been tempered or tempered during its transit.

We can summarize SCADA Protocol attack vectors as below [13]:

- Message spoofing (lack of confidentiality and integrity)
- Message Modification (Lack of confidentiality and Authentication)
- Replay Attacks (lack of integrity)
- MITM attacks (lack of C-I-A)
- Denial of service (affecting availability)

Problems related with Transmission Media

As afore mentioned, SCADA network uses variety of transmission medium such as Radio Links, Telephonic lines or Cables. We know that these communication mediums are prone to the attacks like interception, interruption and/or Denial of Service. For example, now a days it is relatively very easy to crack WEP encryption [14] and even more advanced WPA2 wireless encryption [15]. Any malicious user or hacker may intrude into such network which has SCADA systems in operation thereby, cracking WEP or WPA2 and perform illegal operations as there is no inbuilt security in widely used protocols like Modbus TCP/IP and DNP3.

Vendor specific SCADA problems

There are many vendors which manufactures SCADA products. Major among these are Intellution, Omron, Rockwell, Wonderware, Citect, Siemens, National Instruments etc. Needless to say that SCADA products so manufactured may have some vulnerabilities. Recent example of such product is Siemens PLC operating on Siemens Step7 Software on which a targeted attack was made [16] [17] such that only Siemens PLC gets affected by a worm. The worm was later discovered as stuxnet. Also in [18] authors have successfully validated Replay attacks, Cryptographic attacks, Denial of service and fragmentation attacks on Omron PLC CJ1M-CPU11-ETN and Omron HMI NS5-SQ11-v2. So, there is huge community of malicious people out there who finds weakness or vulnerabilities in SCADA systems and exploits them by various means like malware, control injection [19] etc.

Problems in Auditing SCADA systems

SCADA Systems being different than Business I.T. Systems or Other Traditional Enterprise Systems faces difficulty in Auditing them [20]. Some of the reasons behind these difficulties are as follows:

1. Majority of SCADA systems are put in operation for decades and have unknown security posture.
2. Traditional practices of Auditing like red-teaming, penetration testing and vulnerability assessment proves to be unsatisfactory and also limited in scope as one cannot risk to take out these systems from operation. This may cause devastating effect.
3. No full proof procedure or guidelines are present till date which can be followed effectively while auditing SCADA system.
4. I.T. Auditors having vast experience in Business IT Systems and Other Enterprise Systems usually lack knowledge for SCADA systems and hence are unable to predict the behavior accurately while auditing SCADA systems. For example patching the systems to eliminate vulnerabilities is considered to be a good practice in info sec world but the same can`t be applied to the SCADA systems as patching those systems may open doors for some major vulnerabilities and even harm the SCADA personnel as he/she are direct in contact with such systems.

Problems with SCADA system implementation cycle

As mentioned earlier, most of SCADA systems are kept operational for many years if not many decades and costs huge amount of money for their initial establishment. So, it is very unlikely to change or replace these systems in few years even if some sort of

vulnerability is found. As a result these vulnerable systems keeps always running in vulnerable state till some major/minor disaster happens. One should also remember that applying a patch is not always possible to such systems as their operational behavior can`t be predicted in advance.

III. RELATED WORK DONE TO MITIGATE VULNERABILITIES IN SCADA SYSTEM AND SCADA NETWORK

This section is dedicated to the work done to mitigate certain vulnerabilities in SCADA Systems and SCADA networks. Let`s first talk about the Protocols. As we know that DNP3 and Modbus TCP/IP are widely used protocols in SCADA network so, many work is carried out to secure these protocols. Major among these are [13] and [21]. In [13], author has proposed a unique scheme for securing Modbus TCP/IP protocol which is also backward compatible. Author in [21] have also taken an initiative to secure DNP3 protocol called as flexi-DNP3 protocol. In such approach author has carried out further work from the proposed DNPSec protocol.

As we know that auditing SCADA systems is very difficult and one has to take utter caution while auditing such systems. So, in order to perform such audits and predict the behavior of SCADA system in real environment many test beds have been proposed. Among various such test beds [20] is one of the most practical one. However, author makes use of Omron physical equipment in his work. Thus, it's not a perfectly simulated environment but the combination of Simulated and Emulated environment to get perfect results.

[22] and [10] discusses about the assessment of SCADA networks, [22] mentions functional assessment whereas [10] makes use of attack trees to assess security posture of SCADA network. In [2] author mentions optimization function which is used to reduce SCADA specific vulnerabilities. Some of the important recommendations are mentioned in [8]. Though Intrusion Detection Systems being new to SCADA networks to detect network attacks is discussed from [19] [23] - [25].

IV. DISTINGUISHING SCADA SYSTEMS FROM BUSINESS I.T. SYSTEMS AND C-I-A TRIAD W.R.T SCADA SYSTEMS

Certain properties and characteristics make SCADA systems and SCADA networks different from Business I.T. Systems. Below are some of the points which make them different [26].

1. Unlike business IT Systems, in SCADA systems or other control systems, execution of any logic affects the physical environment and thus the physical safety is of paramount importance while operating SCADA Systems.
2. SCADA systems are time critical systems, even the delay of 1us can cause devastating effect which can also claim human lives. They are also called as Hard Real Time systems which has certain deadline of time to complete its operation.
3. SCADA systems runs 24 X 7, 365 days every year without rebooting. Some are thought of running for decades. So, one tempering such systems can be a great disaster. This is one of the reason why SCADA systems are not properly audited.
4. SCADA system uses RTOS (Real Time Operating System) and such systems are more prone to memory allocation vulnerabilities. Thus, such systems are also more vulnerable to Buffer Overflow attacks.

Given below table briefly summarize all the major differences [27]

Table 1 Difference between SCADA Systems and Business I.T. Systems

Business I.T. Systems	SCADA Systems
Not real-time	Real-time basis
Correctness of Information	Response time is critical
Delay Allowed	Big problems caused by delay
Planned Tasks	Sequential Tasks
Data integrity is important	User`s security is important
Task loss by data corruption	Economic loss and/or casualties
Restoration by re-booting	Continuous operation required.

Understanding the famous C-I-A triad from SCADA`s System/Network perspective. According to SANS institute [28], confidentiality, integrity and availability can be defined as follows:

1. ***Confidentiality:*** Confidentiality prevents all classes of sensitive information from need to know users while makes it accessible to right users having right credentials.
2. ***Integrity:*** Integrity means trueness of data while in transit. It involves maintaining trustworthiness, consistency and trueness of data over its transmission. It`s a property which takes care of data which must not get changed while in transit.
3. ***Availability:*** Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of-service attacks.

As, we know that SCADA systems communicates by transmitting and receiving control signals either in binary form (if it is two-step control device like switch on or switch off, 0 or 1) or analog form (if device needs to regulate speed, temperature, flow etc. within certain level) from MTU`s to RTU`s and vice versa. The control signal information must be strictly following the order of

availability, integrity and confidentiality. Thus, confidentiality is of little or no use to such systems [29]. Whereas on other hand (Business IT Systems) confidentiality is of prime importance.

V. CATEGORIZATION OF SCADA COMPONENTS AS PHYSICAL AND LOGICAL

We have identified major SCADA components as Physical/Logical. This is due to the fact that some components can be touched and felt like HMI and PLC Hardware where as some like Protocols, policies, procedures can`t be felt. So, this would be one of the important factor on which such division is based. Here we only discuss major components both physical and logical which bears more importance then rest. These are components which forms whole SCADA system/network.

Physical Components

1. ***Transmission Medium:***
   SCADA Systems uses various transmission Medium for communication. It may be wired or wireless or sometimes proprietary communication media. One shall consider security in serious manner if SCADA systems are operating with wireless communication medium as one can enter the secure periphery thereby, cracking its WEP or WPA-2 encryption system.
   Remedy: Intrusion Detection System, use of complex password and MAC address binding.

2. ***SCADA Hardware (HMI-PLC):***
   The heart of SCADA system is considered as HMI and PLC. HMI or Human Machine Interface is used by SCADA operator to send control signals for performing certain task. Programmable logic controller receives these signals via communication medium from operator and processes it accordingly. Many times it is found that these SCADA hardware are used in operation with their default configuration. This might lead to disruption of ongoing process as some might accidentally (Employee) or intentionally (Disgruntled employee or any malicious person) change its configuration.
   Remedy: Configure the device properly before making it operable in live environment. One must follow defense in depth mechanism while configuring such devices.

3. ***Integration of Mobile devices in SCADA network*** [8]: Now a day's mobile devices are used for controlling SCADA operations in SCADA network. SCADA system applications are accessed through mobile devices. Such can be an emerging threat and also a new domain for hackers to play with.
   Remedy: Make sure that your Mobile device`s operating system is updated and has good quality Anti-virus/malware software installed. Also the application through which such access is possible shall be thoroughly audited.

4. ***Physical Access to SCADA site:*** One shall also think about the physical security for SCADA site. Only SCADA security personnel shall have access to SCADA site. If such precaution is not taken then some disgruntle employee may enter SCADA site and disrupt their operations.
   Remedy: There must be bio-metric system installed at SCADA site`s entrance which checks credentials for any person willing to enter SCADA site. Placing Security Guards and installing security cameras would be added advantage.

5. ***Integration of SCADA systems with Business IT systems***: All most all SCADA systems are integrated with Business IT systems, and these systems on the other hand are connected to internet. So we can say that SCADA systems are indirectly connected with internet. With enough inclination one can easily cross the secure periphery of Business IT systems and enter into SCADA network from Internet.
   Remedy: Follow defense in depth mechanism and not security by obscurity. Regular and thorough Auditing of Business IT systems and SCADA systems must be done.

Logical Components

1. ***Commercial Off the Shelf COTS Software*** [30]: COTS software also contributes to the lack of security. COTS software indeed is cheaper solution but at the cost of security risk. This is due to the fact that COTS software is not primarily designed for the SCADA systems which leaves some vulnerabilities within the software and need additional security countermeasures.
   Remedy: Patching is the best way to eliminate the risk of exploitation on such software.

2. ***SCADA Protocols:*** Majority of SCADA systems use MODBUS TCP/IP and DNP3 protocol. Both of these protocols are vulnerable to many classes of network attacks like Denial of Service, Man-In-The-Middle MITM, replay attacks etc.
   Remedy: Research has been carried out in this field and now we have secure versions of these protocols. Use these secure version of protocols instead legacy one. But, again there is a problem for already working SCADA system. They can`t be stopped even for single micro second. They must be permanently turned off and more robust system must be placed.

3. ***SCADA application security:*** SCADA application runs on standard computers which in turn runs on various operating systems like Linux and Windows. Such application must be accessed in secure manner.
   Remedy: Install and configure Host Based Intrusion Prevention System to protect such application from getting modified.

4. ***Bandwidth of SCADA network:*** SCADA networks are said to be of minimum bandwidth network. A typical SCADA network operating on Modbus TCP/IP protocol needs as less as 10 MBps bandwidth. This is due to fact that SCADA system works on request/response action carrying small information signals. Sudden increase in bandwidth or fluctuating bandwidth indicates Denial of Service attack.
   Remedy: Network monitoring tools and Network Intrusion Detection and Prevention System can be used to counter such situation.

VI. CONCLUSION

Security among Supervisory Control and Data Acquisition Systems is considered as a hot topic now a days. Earlier SCADA systems were not such which are like today. This is because earlier SCADA systems used to work in stand-alone manner in an isolated environment. Convergence of SCADA systems with traditional IT systems has indeed helped to expand Business and helped to centrally monitor the system but at the cost of lack of security among such systems. Information Security professionals and SCADA personnel have not considered security of such critical infrastructure seriously until the recent incident (2010) that infected almost 14000 computers and Nuclear Plant at Iran by STUXNET worm. SCADA systems being most critical infrastructure systems of any Nation, security of such systems must be thought off in serious manner. In this paper we have shed some light on the working of Modern SCADA systems, its individual components and the way to secure these components. We have also discussed the famous C-I-A triad from SCADA system perspective along with its Technical and Non-Technical problems that current SCADA system faces.

REFERENCES

[1] "SCADA Primer" [Online] Available: http://www.micrologic.com.ph/primers/scada.htm
[2] Kim, S. H., Eom, J. H., & Chung, T. M. (2012, June). A study on optimization of security function for reducing vulnerabilities in SCADA. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 65-69). IEEE.
[3] OFFICE OF THE MANAGER NATIONAL COMMUNICATIONS SYSTEM, "Supervisory Control and Data acquisition (SCADA) systems", October 2004.
[4] "SCADA" [Online] Available: http://en.wikipedia.org/wiki/SCADA
[5] Ashton, Kevin. "That 'internet of things' thing." *RFiD Journal* 22 (2009): 97-114.
[6] "Modbus Protocol Specification" [Online] Available: http://www.modbus.org
[7] "Overview of DNP3 Protocol" [Online] Available: http://www.dnp.org/pages/aboutdefault.aspx
[8] Rautmare, S. (2012, December). SCADA system security: Challenges and recommendations. In India Conference (INDICON), 2012 Annual IEEE (pp. 1-4). IEEE.
[9] "Bureau of Indian Standards" [online] Available: http://www.bis.org.in/index.asp [Dt. 03/04/14]
[10] Byres, Eric, Matthew Franz, and Darrin Miller. "The use of attack trees in assessing vulnerabilities in SCADA systems." *Proceedings of the International Infrastructure Survivability Workshop*. 2004.
[11] Graves, Kimberly. *CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50*. John Wiley & Sons, 2007.
[12] East, S., Butts, J., Papa, M., & Shenoi, S. (2009). A Taxonomy of Attacks on the DNP3 Protocol. In *Critical Infrastructure Protection III* (pp. 67-81). Springer Berlin Heidelberg.
[13] Hayes, G., & El-Khatib, K. (2013, June). Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol. In *Communications and Information Technology (ICCIT), 2013 Third International Conference on* (pp. 179-184). IEEE.
[14] Reddy, S. V., Sai Ramani, K., Rijutha, K., Ali, S. M., & Reddy, C. P. (2010, June). Wireless hacking-a WiFi hack by cracking WEP. In *Education Technology and Computer (ICETC), 2010 2nd International Conference on* (Vol. 1, pp. V1-189). IEEE.
[15] "Cracking WPA/WPA-2" [Online] Available: http://www.aircrack-ng.org/doku.php?id=cracking_wpa
[16] Chen, T. M. (2010). Stuxnet, the real start of cyber warfare?[Editor's Note]. *Network, IEEE*, *24*(6), 2-3.
[17] "The STUXNET Worm" [Online] Available: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf
[18] Sayegh, N., Chehab, A., Elhajj, I. H., & Kayssi, A. (2013, June). Internal security attacks on SCADA systems. In *Communications and Information Technology (ICCIT), 2013 Third International Conference on* (pp. 22-27). IEEE.
[19] Gao, W., Morris, T., Reaves, B., & Richey, D. (2010, October). On SCADA control system command and response injection and intrusion detection. In *eCrime Researchers Summit (eCrime), 2010* (pp. 1-9). IEEE.
[20] Urias, V., Van Leeuwen, B., & Richardson, B. (2012, October). Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. In *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012* (pp. 1-8). IEEE.
[21] Bagaria, S., Prabhakar, S. B., & Saquib, Z. (2011, December). Flexi-DNP3: Flexible distributed network protocol version 3 (DNP3) for SCADA security. In *Recent Trends in Information Systems (ReTIS), 2011 International Conference on* (pp. 293-296). IEEE.
[22] Gao-Wang, L., Wen-Yun, J., & Dong-Yuan, S. (2012, March). Functional Vulnerability Assessment of SCADA Network. In *Power and Energy Engineering Conference (APPEEC), 2012 Asia-Pacific* (pp. 1-4). IEEE.

[23] Shosha, A. F., Gladyshev, P., Wu, S. S., & Liu, C. C. (2011, September). Detecting cyber intrusions in SCADA networks using multi-agent collaboration. In *Intelligent System Application to Power Systems (ISAP), 2011 16th International Conference on* (pp. 1-7). IEEE.
[24] Carcano, A., Fovino, I. N., & Masera, M. (2010, July). Modbus/DNP3 state-based filtering system. In *Industrial Electronics (ISIE), 2010 IEEE International Symposium on* (pp. 231-236). IEEE.
[25] Goldenberg, N., & Wool, A. (2013). Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*, *6*(2), 63-75.
[26] Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing* (pp. 380-388). IEEE.
[27] Kang, D. J., Lee, J. J., Kim, S. J., & Park, J. H. (2009, October). Analysis on cyber threats to SCADA systems. In *Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009* (pp. 1-4). IEEE.
[28] SANS Institute [online] Available: http://www.sans.org [Dt: 25/10/2013]
[29] Zia Saquib (2013, October). Internal Security- Technologies to Pre-empt and Protect. IEEE SCADA Conference, Mumbai Section.
[30] Robles, R., Choi, M. K., Cho, E. S., Kim, S. S., Park, G. C., & Yeo, S. (2008). Vulnerabilities in SCADA and critical infrastructure systems. *International J. of Future Generation and Networking*, *1*(1), 102-103.