Open Architecture Supervisory Control and Data Acquisition System: Security Enhancement with Defense-in-Depth Strategies

Alade, A.A[#1], Ajayi, O.B[*2], Okolie, S.O[#3], Alao, O.D[#4], Akinsanya, A.O[*5], Eze, M.O[#6], Ebiesuwa Seun[#7]
[#1*2#3#4*5#6#7]*Faculty, Computer Science Department, Babcock University, Ilishan-Remo, Ogun State, Nigeria*

***Abstract*—** *The function of the Supervisory Control and Data Acquisition (SCADA) System is to monitor and control physical processes in real time in a geographically spread environment. SCADA system is applied in supervision and control of devices action in electricity distribution, transmission; oil and gas pipelines, water distribution, and traffic lights among other critical infrastructure. Deregulation of electricity sector in Nigeria provides private independent power producers' access to the Transmission Company of Nigeria network and hence transforms the closed (isolated) SCADA System of the TCN to an open architecture SCADA System. An open architecture SCADA System is susceptible to threats and attacks within and without with catastrophic impact on the efficiency of the critical infrastructure it is designed to monitor and control. Using empirical method, the type of threats and level of exposure of the TCN SCADA System were examined. The investigation revealed that TCN SCADA System is majorly protected against internal threats. Hence security enhancement through Defense-in-depth strategies that would provide wide arrays of security were proposed and briefly elaborated on for successful implementation.*

Keywords — *Defense-in-depth, Firewalls, Intrusion Detection System (IDS), Policy and Procedures, Remote Terminal Units (RTU), Risk Assessments, Security Zones, SCADA, Threats and Vulnerability.*

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems provide real time data on industrial process operations, improve its efficiency and reduce operations cost. The use of the emerging advanced communications and computing technologies has aided SCADA's connection to commercial/proprietary networks, though it was initially built for isolated operations (Dayal et al, 2015).

It comprises the master station that is connected to several Remote Terminal Units (or RTUs) and the field data through a communication system. The data acquired from the field devices through the RTUs are displayed by the master and used by the operator toperform control tasks remotely. Optimization of the plant operation is achieved through the timely and precise data from the field (Bailey et al, 2003). According to SIEMENS (2013), some of the areas of SCADA application are:

Supply network of utilities and regional public utilities (gas, electricity, water, sewage, thermal heat transfer); Switchgears of national power utilities; supply networks of public local traffic companies (railways, subways, buses and local traffic).

Installations in the buildings for escalator, illumination, air condition, heating etc.

It is also applied in processing of water (sewage) and managing of water reservoirs; chemical and petrochemical installation and pipelines.

This paper focuses on SCADA System application in the power system of the Transmission Company of Nigeria (TCN). Integration of the above described isolated legacy SCADA System of the company with the internet, enterprise network/intranet and SCADA Systems of power stations, transmission, distribution companies and other similar utilities within and outside the country results in an open architecture or hybrid network SCADA System which is fraught with series of security challenges.

As depicted in Fig. 1, Zone 1 represents the Internet, external SCADA Operations facility and vendor networks. Zone 2 is the field devices that comprise the sensors, Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs); Zone 3 is the SCADA System master station while Zone 4 is the Corporate LAN. Security challenges increase with integration of Zone 1 with Zone 3 and 4 resulting in an open SCADA architecture which is exposed to both internal and external threats.

II. BACKGROUND TO THE RESEARCH

More than ever before, some of the most critical national infrastructure such as oil processing facilities, nuclear power stations, electric power grid, water pumping and waste treatment systems are under various threats, especially, terrorism and willful acts of sabotage. Threats to the essential infrastructure are boundless – both developed and developing nations of

the world are vulnerable. Attack on these important facilities of modern living could cause fatality, services disruption, equipment malfunction, environmental disasters and colossal financial losses. Security of SCADA systems that control these facilities requires utmost attention. This was summed up by Shea (2004): "The potential consequences of a successful cyber-attack on critical infrastructure industrial control systems range from a temporary loss of service to catastrophic infrastructure failure affecting multiple states for an extended duration".

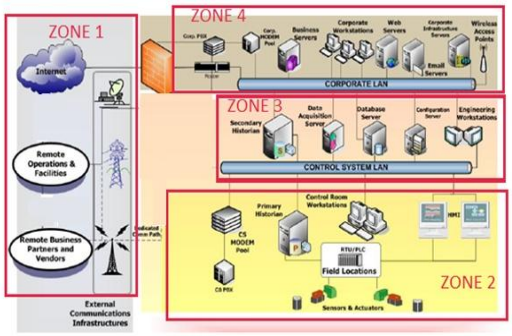

Fig. 1: Isolation of control and corporate domains (Traditional) *(Source: U.S. Home Land Security, 2009)*

The traditional SCADA System is isolated (closed) from other communication network; hence, its security is limited to as access control protection against local intruders, the insiders. Security measures such, authorization and passwords feature in the closed traditional SCADA System. With open architecture SCADA System that connects both the enterprise/intranet network and foreign SCADA System, the threats increase, necessitating a different dimension of security measures. It should be stated that the global dimension of sabotage and attack on critical infrastructure neither spares the erstwhile segregated nor the open architecture SCADA System.

With this background in view, the author examines the security in place in Transmission Company of Nigeria SCADA System and proffer solutions to its enhancement.

III. Literature Review

Queiroz et al (2011) came up with a tool for simulating SCADA that supports inclusion of external devices. The paper submitted that SCADA Systems have no immunity against cyber attacks and that critical infrastructure is under greater threats than that which the common computers are exposed to. The authors cited an example of threat to SCADA System in Maroochy Shire, Queensland where the sewage system was attacked resulting in release of 800, 000 litres of sewage that spilled out into local parks and rivers Another example cited in the paper was Davis-Besse nuclear Power in Oak Harbour, Ohio. The system monitoring the safety of the plant was disabled for about 5 hours following the attack of Slammer SQL server worm.

FORTINET (2010) reported that "The highly advanced Stuxnet worm discovered in 2010, which includes the capability to reprogram PLCs hide the changes, is the first worm known to specifically target SCADA systems and critical industrial infrastructure. It was digitally signed with two authentic stolen certificates, making it difficult to detect, and could be upgraded remotely via peer to peer networking. Stuxnet used Windows vulnerabilities as the vector for infection, comprising multiple computers in the network via the host operating system. The virus payload was specifically targeted at interacting with SIMATIC WinCC and SIMATIC Siemens STEP 7 industrial process control systems and further more at motors running at a certain frequency, a very specific target"

Tang (2009) defines SCADA and related control system such as Industrial Control System (ICS) - examples are Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs). The author then described the components of SCADA System. He categorized cyber attacks into three: intentional attacks, unintentional consequences or damage caused by viruses, worms, control system or by insider or mechanism. Nine (9) incidents of cyber attacks that occurred between 1999 and 2008 were listed. One of them was "the hatch Nuclear Power Plant shutdown in Georgia, U.S.A". This occurred while the plant's business network was being updated. The paper also identified the following attack vectors on SCADA System:

1. "Back door and holes in network perimeter
2. Vulnerabilities in common protocols
3. Database attacks
4. Communications hijacking and "man-in-the middle" attacks."

In all the papers reviewed, little attention was placed on specific defensive actions that would protect SCADA System and hence critical infrastructure against cyber attacks. It is this identified gap that this paper intends to fill by studying the extant security measures in place on Transmission Company of Nigeria SCADA System and ultimately recommend defense-in-depth strategies as solutions to SCADA System security problem.

IV. Significant Cyber Threats

Kang et al (2009), in their paper entitled "Analysis on Cyber Threats to SCADA Systems" compiled a comprehensive list of probable threats to SCADA Systems (Table 1 below). The paper observed that the list is not exhaustive.

This research centers on strategies that would offer total defense to the critical infrastructure of power system against the list of common computer threats to both isolated and open architecture SCADA System with the "Transmission Company of Nigeria" network as a case study.

TABLE I: COMMON COMPUTER THREATS *(SOURCE: KANG ET AL, 2009)*

1	Authorization Violation	9	Information leakage	17	Sabotage	25	Traffic Analysis
2	Bombs (Logic or Time)	10	Intercept/Alteration	18	Scavenging	26	Trap Door/Back Door
3	Browsing	11	Interference with Database, Query, Analysis	19	Spying	27	Trojan Horse
4	Bypassing Controls	12	Masquerade	20	Service Spoofing	28	Tunneling
5	Data Modifications	13	Physical intrusion	21	Sniffers	29	Unauthorized Access violations of Permission
6	Denial of Service	14	Replay	22	Substitution	30	Unauthorized Access Piggybacking
7	Eavesdropping	15	Repudiation	23	Terrorism	31	Virus
8	Illegitimate Use	16	Resource Exhaustion	24	Theft	32	Worm

V. METHODOLOGY

The variables of interest were threats, vulnerability and defense. SCADA System of the Transmission Company of Nigeria is manned by a few number of personnel specially trained in Computer Science, engineering and System management. The researchers were conducted round the TCN SCADA facilities. Questionnaires were administered to the technical personnel to determine the level of their knowledge and awareness of cyber threats, general security issues and the types that they once experienced, etc. Apart from the general cyber threats, the questionnaire administered, also identified peculiar threats to an open SCADA System.

For the purpose of the research there was full access to the Control Centre's supervising, monitoring and data archiving computer servers such as:

1. Human Machine Interface (HMI) servers
2. Communicator servers
3. Historical servers
4. Tele-control interface servers
5. Administrator servers
6. Remote Terminal Units

VI. COMPARISON OF INTERNAL AND EXTERNAL THREATS TO SCADA SYSTEMS

In the course of this study, the researcher wanted to know if all external and internal threats were intentional. The response from the questionnaires revealed that most external threats were intentional and specific. Its intention is usually to cause havoc, operational failure and financial loss. Sabotage and act of terrorism with the devastating consequence (impact) of loss of assets and abrupt disruption of services are examples of external threats to an open SCADA System. As in the case under study, communication infrastructure between zone 1 and Zone 3 (fig. 1.) from a far distance might be the target of attack in order to perpetrate an external attack.

Compromise of passwords and access rights may give an inexperience staff access to the vital system files. In the process, the files could be unintentionally corrupted, modified or deleted, resulting in malfunction of the SCADA System.

It was, however, found out that internal threats could be both intentional and unintentional. Examples of internal threats that are intentional are those perpetrated by unsatisfied staff of an organization. Such staff members know the in and out of the Systems and due to frustration or discontent, they may intentionally exploit the vulnerable part of the SCADA System. Unintentional threats manifest in different ways – use of infected portable discs such as flash discs, compact discs, tape, etc could introduce malware into the System.

VII. RISK, VULNERABILITY, THREATS AND IMPACTS

Risk, vulnerability, threat and impact are defined as follows:

1. "Risk is the likelihood that something bad will happen that causes harm to informational assets or loss of assets.
2. Vulnerability is a weakness that could be used to endanger or cause harm to informational assets.
3 A threat is anything (man-made or act of nature) that has the potential to cause harm.
4 When a threat does use a vulnerability to inflict harm, it has an impact".

In information security, the impact is a loss of availability, integrity and confidentiality and possibly other losses (loss of income, loss of life and real property).

VIII. FINDINGS – EXISTING SECURITY MEASURE IN PLACE ON TCN SCADA SYSTEM

Security requirements already considered in the TCN SCADA Investigation revealed that the present Transmission Company of Nigeria (TCN) SCADA System has security built into it, especially, the administrative and physical controls. Logical controls such as passwords and access rights are also in place. These, however, need to be reviewed, reinforced and updated to take care of the impacts of threats that are possible through the internet, intranet and SCADA Systems of

other utilities that are integrated to the SCADA System. System centered on the following:

1. Confidentiality: This is assured through data encryption and use of password. Through this, important information being broadcast such as 'emergency shutdown', 'equipment outage', 'fire alarm', etc, are encrypted.

2. Integrity: According to Coi, et al (2009), it is critical that messages being transmitted from one node to another "are not tampered with and that no new message is inserted as message modification and injection can cause huge damage" to electricity and critical infrastructure. Sufficient measure is already built into the SCADA System to ensure this.

3. Availability: Importance of System availability cannot be overemphasized. Unavailability of services in the shortest possible time "can cause physical damage or threaten human life". Hence, the TCN SCADA System is designed with this in view.

4. Access Control: The TCN SCADA System's design takes issue of access control into consideration. An unauthorized agent is denied access to every control system resources. "Multi-layer access control, device access control and physical access control" are considered.

5. Network Security: Interface of the TCN SCADA System with other network due to integration with internet, intranet and SCADA Systems of other utilities poses a tremendous security challenge. This is the main focus of this research work. That is, how to mitigate the risks posed by exposure of the closed TCN SCADA System as mentioned above.

6. Security Policy: Security policy such as password policy, security plan, risk analysis, recovery plan and auditing are already in place. The TCN SCADA System's password policy is investigated against the standard recommended in a clause from ISO 17799 standard. According to the standard, "a password management system should among others:

- enforce the use of individual users IDs and passwords to maintain accountability
- allow users to select and change their own passwords and include a confirmation procedure to allow for input errors
- enforce a choice of quality passwords
- force users to change temporary passwords at first login
- maintain record of previous passwords to prevent re-use
- not display passwords on the screen when being entered
- store password files separately from application system data
- store and transmit passwords in protected form (e.g. encrypted or hashed)".

IX. PROPOSED REINFORCEMENT: DEFENSE-IN-DEPTH STRATEGIES

"Defense-in-depth (also known as Castle Approach) is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system" (Stewart, et al, 2015). The concept involves strengthening of system security in multiple of layers rather than depending solely on perimeter defense by the use of firewall.

Application of defense-in-depth strategy ensures that in event of failure of one defense measure, another is in place to continue with thr protection. Defense-in-depth, unlike the perimeter firewall, is not a product that can be bought in a shelf. It is rather a security arrangement that has layers that are responsible for diverse aspect of security of SCADA System integrated with both corporate network /internet. Defense-in-depth has been approached by diverse authors and technology-tools providers in different ways. As contained in table 2.and illustrated in Fig. 2, seven layers of defense are proposed. All other layers of defense would have been penetrated and weakened before data layer, the innermost is reached.

TABLE 2. DEFENSE-IN-DEPTH LAYERS *(Source: Paloma, 2007)*

LAYER	DESCRIPTION
1	Policies, procedures and awareness
2	Physical
3	Perimeter
4	Internal Network
5	Host
6	Application
7	Data

A. Defense-In-Depth Layers

The distinguished characteristics of each layer of the defense-in-depth are:

1) Layer 1: Policies, procedures and awareness

This layer requires that the organization establishes well documented security policies to be pursued in order to secure the infrastructure and the SCADA System. Policy should include access rights of personnel to the physical infrastructure and to a part of the SCADA soft and hardware. Strategies to trace intruders, determine rate of security assessment, risk analysis, should be highlighted among other policies (U.S. Home Land Security, 2009). Other consideration includes: Documenta-

tion of Standard procedures to follow when handling SCADA System equipment in order to prevent unscheduled outage or equipment breakdown (Kuipers and Fabro, 2006).

In case of compromise of a computer on the network, an incident response procedure is kept to teach the employees on the necessary sequence of actions.

Creation of awareness among all levels and classes of technical and non technical personnel about the importance of the SCADA System, its vulnerabilities and the need to safeguard it from varied possible threats and subsequent attacks. It needs be clear to every personnel the catastrophic impact of its attack, emphasizing that huge financial loss, critical service interruption and fatality might result. It should be made clear to the personnel that vital information about the SCADA System or any of the servers should not be divulge to the outsiders.

Ensure that all requests for information are directed to responsible officers in the central security location for evaluation prior to approval.

Training of every level of personnel – the executive, managers both technical and non-technical and others, is necessary in order to ingrain the sense of security of this sophisticated supervisory tools in them. Both formal and informal training on cyber and industrial control systems security, situation management and response actions during emergency are highly essential. (Fabro and Nelson, 2007).

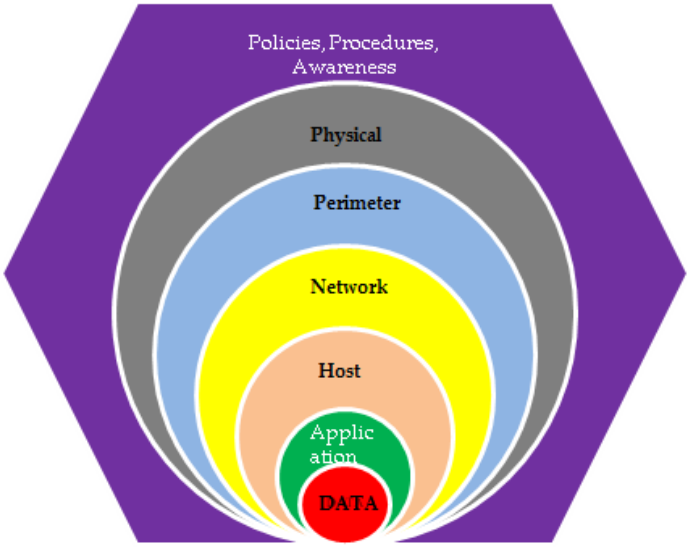

Fig. 2: 7 Layers of Defense-in-Depth *(Source: Paloma, 2007)*

2) *Layer 2: Physical*

The physical layer include infrastructure, computer hardware and network, telephone cables, optical fibres, wired/unwired access points, micro wave/radio equipment both local and remote sites that are connected with the SCADA network.

Means of securing the above listed constituents of physical varies. Assets such as organization wall fence, administrative and industrial building would require intruder detection devices such as closed circuit television and alarm triggered sensors to monitor and alert in case a saboteur intends to gain unauthorized access to the SCADA facility. Control of access to the building begins right from the entrance main gate to the control system building and specific rooms that host the critical equipment. Apart from the control of personnel, visitors into the premises must be adequately monitored. Physical elements like optical fiber cables can be secured against the menace of an attacker by embedding it in protective ducts or inside electricity transmission conductor.

3) *Layer 3: Perimeter*

Network dictionary.com defines "A network perimeter"as "the boundary between the private and locally managed-and-owned side of a network and the public and usually provider-managed side of a network". The integrated networks shown in Fig. 3 is segmented into four networks: Zone 1 that consists of the internet, remote operations/facilities and business network; Zone 2 has the field bus sensors, devices and remote terminal units/Programmable Logic Controller; Zone 3 is made up of the Control System LAN and the associated computer servers for various data analysis functions while Zone 4 is the corporate LAN with the attached computer systems, printers, scanners, etc.

The network perimeter is usually protected by deploying firewalls that provide extra levels of defense between different networks. Installed along with the firewalls is Intrusion Detection Systems (IDS). This is, however, a combination of products (a set of tools and processes) that offer network monitoring services which provide the system administrator information on the network usage activities (Snyder). By implementing IDS one is warned ahead of threats to the network with ample opportunity to put a countermeasure in place.

With the exception of zones 2 and 3 that form the isolated or closed SCADA System architecture, other zones have little or no interaction prior to integration. With integration, perimeter security will be required between the boundaries of:
Zone1/Zone 4 – both Firewall and Intrusion Detection System would be required between the Internet and the Corporate LAN. (Fig. 3). Zone 1/Zone 3 – comprises – both Remote Operation & Facilities and Remote Business Partners & Vendors pass through the Firewall and Intrusion Detection System. (Fig. 3)

4) *Layer 4: Internal Network*

In addition to securing the SCADA network with appropriate firewalls and Intrusion Detection/prevention

Systems, hardening of the networks is recommended (Pauna and K. Moulinos, 2013), (U.S. Department of Energy, 2010). This simply means disabling of unnecessary services. As much as possible idle services / equipment should be removed. Removal of such idle services would reduce the vulnerability of the network nodes. This is particularly necessary in an integrated SCADA System where the control system is linked with the Corporate LAN and Internet.

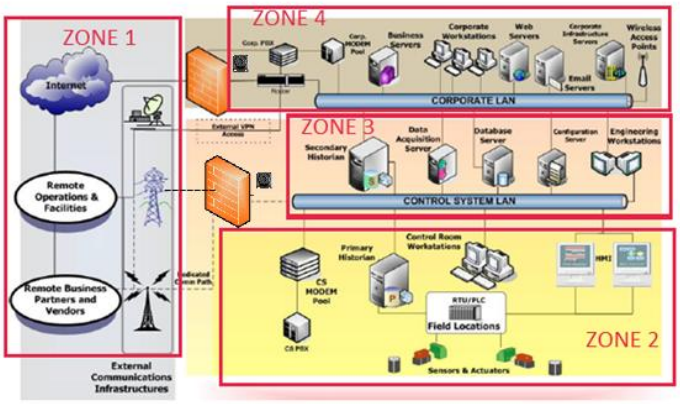

Fig. 3: Integrated SCADA Networks *(Source: U.S. Home Land Security, 2009)*

High caution should be exercised in order to ensure that vital network services are not irredeemably disconnected as that might pose a serious problem to the control network with attendant cost.

5) *Layer 5: Host*

The control computer servers and corporate computers are usually protected by host firewalls and other antivirus software. Through the rule sets created by the firewalls, it is able to track the incoming and outgoing traffic on the system. It decides which traffic to allow or deny. Modern day computer systems have the firewall pre-installed to protect their operating system so that it can always be secured against outsiders' attacks.

6) *Layer 6: Application*

This contains authentication, authorization and audit software. The current security arrangement in place on the TCN SCADA system authentication, authorization and auditing among others.

7) *Layer 7: Data*

SCADA System data are very vital. Its corruption could be catastrophic with consequent loss of lives, finance and assets. It is hence important to secure the data from all forms of probable attacks listed above. Having adequately implemented the various layers of defense-in-depth, it would be very difficult to get across to data. However, it is best practice to still secure the data by installing strong anti-virus software on the servers and workstation that are networked with the SCADA System.

X. Regular Risk Assessment and Management

As new technology to tackle security problem emerges so also new threats surface. It is hence necessary that an organization conduct risk assessments of its network regularly to determine the extent of its vulnerability (Guillermo et al, 2010).

Risk assessments require 7 systematic approaches as recommended by ASIS International Guidelines Commission. These are according to ASIS International (2004):

1. Understand the organization, personnel and assets at risk.
2. Specify risk/vulnerabilities.
3. Establish the probability of risk and frequency of events.
4. Determine the impact of the events.
5. Develop mitigation options
6. Study the feasibility of implementation of options
7. Perform a cost/benefit analysis".

Following this, the organization devises detailed management procedures that would guarantee minimization of the impact on the organization whatever the degree of attack.

XI. CONCLUSION

It is obvious from this study that a simple security arrangement in place on the SCADA System of TCN is grossly inadequate to secure an integrated SCADA network that interfaces with Internet/Corporate LAN and outside SCADA systems against the potential threats through the various areas of its vulnerability.

Defense-in-depth security strategies that provide layers of defense which are very difficult to penetrate through are proposed and discussed in the paper.

Defense-in-depth topic is very wide and has extensive dimension with new innovation emerging daily. A comprehensive and detailed work on approaches and implementation strategies for a robust defense for SCADA System are open areas for further researches.

REFERENCES

[1] ASIS International (2004). General Security Risk Assessment Guidelines. Available at www.tisp.org/index.cfm?pk=download&id=10948&p id=10261.

[2] D. Bailey and E. Wright. *Practical SCADA for Industry*. Elsevier Linacre House, Jordan Hill, Oxford OX2 8DP 200 Wheeler Road, Burlington, MA 01803, 2003.

[3] D. Choi, H. Kim, D. Won and S. Kim. An Advanced Key-management Architecture for Secure SCADA Communications. *IEEE Transactions on Power Delivery*, vol. 24, pp. 1154 – 1163, 2009

[4] A. Dayal, A. Tbaileh, Y. Deng and S. Shukla. Distributed VSCADA: An Integrated Heterogeneous Framework for Power System Utility Security Modeling and Simulation. *Proc. IEEE Symp. Modeling and Simulation of Cyber-Physical Energy Systems* (MSCPES' 15), pp. Apr. 2015, doi: 10.1109/MSCPES. 2015.7115408. (Workshop Proceedings)

[5] M. Fabro and T. Nelson. *Control Systems Cyber Security: Defense- in-Depth Strategies*. US department of Home Security Idaho National Laboratory, 2007

[6] FORTINET Incorporated. *Securing SCADA Infrastructure*. White paper, WP-SCADA-R1, 2010.

[7] F. Guillermo, D. Thornton, D. and J. Dawson. *Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems*", Jacksonville State University Jacksonville, AL 36265 USA, 2010

[8] D. Kang, J. Lee, S. Kim, and J. Park. Analysis on Cyber Threats to SCADA Systems. *IEEE T&D*, 1– 4, 2009

[9] D. Kuipers and M. Fabro (2006). *Control Systems CyberSecurity: Defense- in-Depth Strategies*. US department of Home Security Idaho National Laboratory Network Perimeter, available at http://searchnetworking.techtarget.com/definition/

[10] J. Paloma (2007). Windows Server 2008 in an Organization's Defense in Depth Strategy. Available at https://technet.microsoft.com/en-us/library/cc512681.aspx.

[11] A. Pauna and K. Moulinos. Window of exposure… a real problem for SCADA systems? Recommendations for Europe on SCADA patching. European Union Agency for Network and Information Security, www.enisa.europa.eu, 2013

[12] C. Queiroz, A. Mahmood and Z. Tari. SCADASim – A framework for Building SCADA Simulation. *IEEE Transactions on SMART GRID*, vol. 2, 589 – 597, 2011

[13] D.A. Shea. *Critical Infrastructure: Control Systems and Terrorist threat*. Congressional Research Service, the Library of Congress, CR, 1 – 9, 2004

[14] SIEMENS. SICAM ERTU Basic Training Course, Edition: December 2013, PTD SE

[15] J. Snyder. *Six Strategies for Defense-in-Depth Securing the Network from the Insideout*, OPUS, 2014

[16] R. Tsang. *Cyber Threats, Vulnerabilities and Attack on SCADA Network. International Journal of Critical Infrastructure Protection*, 2, 1 – 23, 2009

[17] U.S. Home Land Security. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, 2009

[18] U.S. Department of Energy. *21 Steps to Improve Cyber Security of SCADA Networks*, 2010