Volume 6, Issue 5
October 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Analysis and Planning of the Cyber Security of SCADA Networks

Mohamed Najeh Lakhoua
The National Engineering School of Carthage, University of Carthage,
Research Unit: Signals & Mechatronic Systems, Tunisia
E-mail: MohamedNajeh.Lakhoua@ieee.org

ABSTRACT

The increasing dependence of critical infrastructures and industrial automation on interconnected physical and cyber-based control systems has resulted in an increasing and previously unpredicted cyber security threat to supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs). This work presents a review on SCADA cyber security and the case for improving security to SCADA systems. It examines the factors that have contributed to the growing vulnerability of control systems, and presents new standards designed to protect critical infrastructure including the use of encryption and authentication for SCADA systems. A comprehensive model for analysis and planning of the cyber security of SCADA networks is presented.

Keywords: SCADA, critical infrastructures, cyber security, analysis and planning

1. INTRODUCTION

SCADA systems support our critical infrastructures such as electrical power generation, transmission and distribution, oil & gas transport, and water supplies. The primary purpose of SCADA systems is to monitor and control infra-structure equipment. The Sandia interpretation of the terms PCS and SCADA include the overall collection of control systems that measure, report, and change the process. Essentially, any subsystem that electronically measures state alters process control parameters, presents /stores/communicates data, or the management thereof is subsumed in our definition of SCADA.

Most critical infrastructure, including major utilities infrastructure, industrial networks and transport systems, are controlled by supervisory control and data acquisition (SCADA) systems [1] [2]. In fact, a typical control system consists of one or more remote terminal units (RTU) connected to a variety of sensors and actuators, and relaying information to a master station (Figure 1).

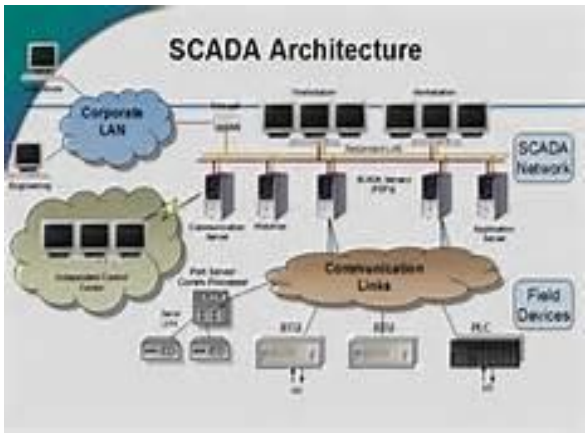

Figure 1. Architecture of SCADA system.

SCADA provides management with real-time data on production, operations, implementations more efficient control paradigms, improves plant and personnel safety, and reduces costs of operation. These benefits are made possible by the use of standard hardware and software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet [3] [4].

SCADA systems are required to deal with increasingly complex and critical situation. They must constantly evolve towards integrated decision making and policy driven by cyber security requirements [5] [6].

The main challenges facing current and modern SCADA systems are complexity, scalability, security, reliability, flexibility, interoperability, robustness, and legacy systems. There have been a lot of proposed security approaches for SCADA system [7] [8]. Every security provider uses different kinds of security strategies for instance authentication, authorization, confidentiality, integrity, non-repudiation. Attacks on such infrastructure may have catastrophic impact and hence the mitigation solutions for the attacks are necessary (Figure 2).

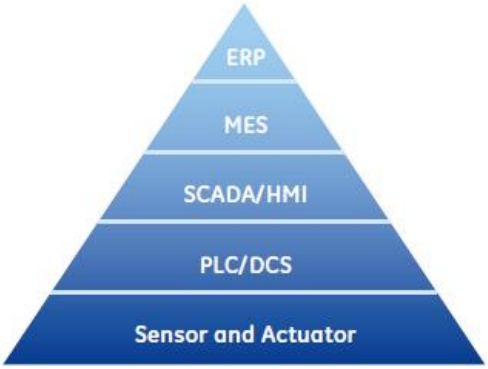

Figure 2. Functionality of a SCADA system.

This paper provides a review of the literature to date on SCADA cyber security for critical infrastructures. It proposes a comprehensive model for analysis and planning of the cyber security of SCADA networks.

Volume 6, Issue 5
October 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

2. ANALYSIS AND PLANNING OF SCADA CYPER SECURITY

As information and communication networks are highly interconnected with the power grid, cyber security of the SCADA system has become a critical problem in the electric power sector. By exploiting the vulnerabilities in cyber components and intruding into the local area networks of the control center, corporation, substations, or by injecting false information into communication links, the attackers are able to eavesdrop critical data, reconfigure devices, and send trip commands to the intelligent electronic devices that control the system breakers. Reliability of the power system can consequently be impacted by various cyber attacks (Figure 3).

Figure 3. Phases of the SCADA cyber security.

In fact, SCADA system plays the most important roles in the remote surveillance system. The development of the communication system of the new substations such as renewable energy sources, smart grid houses, new energy sources in power network, increases the nodes in a data communications network, which increases the number of possibilities to connect to the SCADA system [9].

The security of system that monitor critical infrastructure are vital. The possibility of critical infrastructure services being disrupted would have a significant impact on the wider society as it involves energy, water, gas, transport, and many more utilities [10].

For reasons of efficiency, maintenance, and economics, data acquisition and control platforms have migrated from isolated in-plant networks using proprietary hardware and software to PC-based systems using standard software, network protocols, and the Internet [11] [12]. The downside of this transition has been to expose SCADA systems to the same vulnerabilities and threats that infection Windows-based PCs and their associated networks.

SCADA systems that tie together decentralized facilities such as power, oil, and gas pipelines and water distribution and waste water collection systems were designed to be open, robust, and easily operated and repaired, but not necessarily secure [13] [14] [15]. The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between SCADA systems, office networks, and the Internet has made them more vulnerable to types of network that are relatively common in computer security. “Security by obscurity” is no longer an option for SCADA security [16] [17].

SCADA systems are a network presence and face significant threats and vulnerabilities. SCADA systems were not initially intended to operate within the enterprise environment (Figure 4). Another issue is the inability within SCADA components to deal with the exposure to viruses, worms, and malware that are commonplace today within the enterprise network [18] [19].

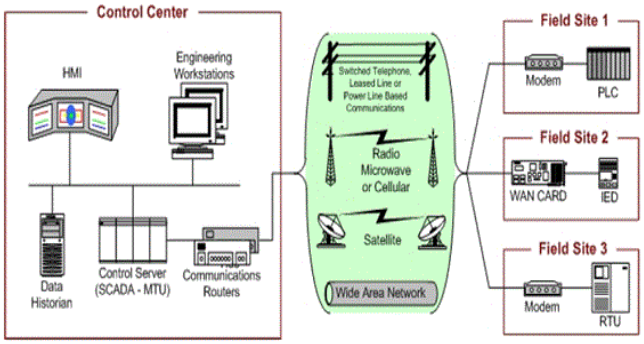

Figure 4. SCADA network.

In order to analyze the cyber security of SCADA network, we use the OOPP (Objective Oriented Project Planning) method [20].

In fact, the OOPP method is considered like a tool of communication, analysis and scheduling of project, whatever is its nature, its situation, its complexity and its sensitivity [21] [22]. This method is used more and more by several financial backers (World Bank, European Union, bilateral Cooperation…) [23] [24]. It is also used to take to terms of development projects, of cooperation (Germany, Canada, Belgium...) or other. It gave a good satisfaction at the time of its exploitation and several researches have been done very well to develop tools and to prove its strength for the scheduling of projects. The descriptive documentation of the OOPP method, indicate that the logic of the OOPP method is not limited in principle to a type of determined problematic [25] [26]. Nevertheless, in practice the method is more appropriated to the following interventions: projects of the technical cooperation and projects of investments with economic and / or social objective.

The OOPP method constitutes a tool of a global systemic modeling enabling to analyze a complex situation by a hierarchically decomposition until reaching an elementary level allowing an operational planning. This method, widely used in the planning of complex projects, involves many operators and partners [27] [28].

Table 1 presents the results of the planning and analysis based on the OOPP method.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Table 1. Model of analysis and planning of the cyber security of SCADA network based on OOPP method.

N°	Code	Activity
1	OS1	**Steps to improve cyber security of SCADA network analyzed**
2	R1.1	Identify steps focus on specification to be taken to increase the security of SCADA networks
3	A1.1.1	Identify all connections to SCADA networks
4	A1.1.2	Disconnect unnecessary connections to the SCADA network
5	A1.1.3	Evaluate and strengthen the security of any remaining connections to the SCADA network
6	A1.1.4	Harden SCADA networks by removing or disabling unnecessary services
7	A1.1.5	Do not rely on proprietary protocols to protect your system
8	A1.1.6	Implement the security features provided by device and system vendors
9	A1.1.7	Establish strong controls over any medium that is used as a backdoor into the SCADA network
10	A1.1.8	Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring
11	A1.1.9	Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns
12	A1.1.10	Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security
13	A1.1.11	Establish SCADA “Red Teams” to identify and evaluate possible attack scenarios
14	R1.2	Identify steps focus on management actions to establish an effective cyber security program
15	A1.2.1	Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users
16	A1.2.2	Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection
17	A1.2.3	Establish a rigorous, ongoing risk management process
18	A1.2.4	Establish a network protection strategy based on the principle of defense-in-depth
19	A1.2.5	Clearly identify cyber security requirements
20	A1.2.6	Establish effective configuration management processes
21	A1.2.7	Conduct routine self-assessments
22	A1.2.8	Establish system backups and disaster recovery plans
23	A1.2.9	Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance
24	A1.2.10	Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls

Volume 6, Issue 5
October 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

3. REVIEW ON SCADA SYSTEM AND CYPERSECURITY

Historically, security concerns over control systems were limited to physical attacks. SCADA system operators rationalized that if the management consoles were adequately isolated and only authorized personnel had access to the network, the system was intrinsically secure. There was little risk of tampering since few people had technical expertise of the system and the data communication paths remained isolated.

In this part, we present some studies of the SCADA cyber security for critical infrastructures that have been presented in various researches:

Researchers Ghaleb and al. [29], have explained that the number of reported cyber security incidents on SCADA systems increased significantly in the past few years. One contributing factor is the fact that security testing of live SCADA systems is not practical as such systems are expected to be operational 24/7. Also and most importantly, conducting live security testing on these types of systems is generally costly. A practical and cost-effective solution is to carry out security testing on a simulated version of the physical setting. The main contribution of this paper is to present a SCADA simulation environment (SCADA-SST) suitable for security testing. The simulation environment is generic, easy to setup (comes with a detailed manual), and supports hybrid architectures (involving simulated as well as physical components). They show how SCADA-SST can be used to simulate two realistic settings, namely, Water distribution and Electrical power grid. Finally, for the sake of security testing example, we show how SCADASST can be used to assess the resilience of common SCADA nodes to DOS attacks.

Researcher Chromik and al. [30], have explained that SCADA networks are an essential part of monitoring and controlling physical infrastructures, such as the power grid. Recent news items show that tampering with the data exchanged in a SCADA network occurs and has severe consequences. A possible way of improving the security of SCADA networks is to use intrusion detection systems. By monitoring and analysing the traffic, it is possible to detect whether information has a legitimate source or was tampered with. However, in many cases the knowledge of just the traffic is not enough. Detecting intrusions could be improved by including awareness about the physical processes that are controlled. This paper shows a simple analysis of a small scenario of a power distribution system, to illustrate the benefits of including the knowledge about the process in detecting breaches in SCADA.

Researcher Almalawi and al. [31], the authors have explained that SCADA systems have become a salient part in controlling critical infrastructures, such as power plants, energy grids, and water distribution systems. In the past decades, these systems were isolated and use proprietary software, operating systems, and protocols. In recent years, SCADA systems have been interfaced with enterprise systems, which therefore exposed them to the vulnerabilities of the Internet and the security threats. Traditional security solutions (e.g., firewalls, antivirus software, and intrusion detection systems) cannot fully protect SCADA systems, because they have different requirements. This paper presents an innovative intrusion detection approach to detect SCADA tailored attacks. This is based on a data-driven clustering technique of process parameters, which automatically identifies the normal and critical states of a given system. Later, it extracts proximity-based detection rules from the identified states for monitoring purposes. The effectiveness of the proposed approach is tested by conducting experiments on eight data sets that consist of process parameters' values. The empirical results demonstrated an average accuracy of 98% in automatically identifying the critical states, while facilitating the monitoring of the SCADA system.

Researcher Singh and al. [32], the authors have explained that cyber-attacks from terrorist, national enemies, disgruntled employees are on the rise now on an Oil Refineries, on shore petroleum fields, off-shore Platforms, Oil and Gas Pipe Lines which will have a catastrophic impact on oil production and in turn on economy of the country, it can also cause serious damage to the environment living being, and even human lives. There is a dire need to protect Petroleum Oil &Gas Processing Infrastructures, Chemical Industry, Nuclear Power Stations, Water pumping & Waste treatment Plants, Electric Power Grids by using a Data Security System, similar systems are in place in Australia, Canada, America and other countries. Current trend of SCADA system protection is to perform backups, upgrade incremental capabilities each year without impacting 24/7 operations and train the personnel regularly, whenever up gradation is carried out. SCADA system should be operated over a Utility Intranet and isolated from public Internet by means of Firewalls, and Routers. It should have a protection based on dynamic predictive mechanism rather than reactive.

Researchers Czechowski and al. [33], have presented the problem in designing the new substation that no one takes into account the aspect of cyber security. This is limited only to choose the mode of communication in the station and method of communication to SCADA system. However, the IEC 60870-5-104 protocol transmits messages in clear text without any authentication mechanism. Furthermore, the IEC 60870-5-104 protocol is based on TCP/IP, which also has cyber-security, issues itself is presented.

Researchers Singh and al. [34], have proposed a testbed that can simulate power systems SCADA. The testbed consists of traffic generator, simulated devices like RTUs, MTU, HMI etc. and the communication channel wrapped around industrial communication protocols such as IEC-60870-5-101 and DNP3. The proposed testbed includes with a comparator module which helps in detecting potential intrusions at RTU. A compromised RTU can be manipulated to send fabricated commands in the grid or to send polled responses from the grid. Detecting compromised systems at early stages helps in reducing damage to Industrial Control System (ICS) and providing higher security measures.

Researchers Zhang and al. [35], have considered four attack scenarios for cyber components in networks of the SCADA system, which may trip breakers of physical components. Two Bayesian attack graph models are built to illustrate the attack procedures and to evaluate the probabilities of successful cyber attacks. A mean time-to-compromise model is modified and adopted considering the known and zero-day vulnerabilities on the cyber components, and the frequencies of intrusions through various paths are estimated. The simulation results demonstrate that the power system becomes less reliable as the frequency of successful attacks on the cyber components increases and the skill levels of attackers increase.

4. CONCLUSION

SCADA systems control some of the most vital infrastructure in industrial and energy sectors, from oil and gas pipelines to nuclear facilities to water treatment plants. Critical infrastructure is defined as the physical and IT assets, networks and services that if disrupted or destroyed would have a serious impact on the health, security, or economic wellbeing of citizens and the efficient functioning of a country's government.1 One does not have to look far for examples of disruptions that have cost organizations time, resources, and possibly lives.

Added to this is the fact that many SCADA systems are vulnerable. It is therefore imperative that system security and risk mitigation be at the forefront of the minds of all SCADA system users.

Cyber-attacks are now becoming a big threat in internet world. Being connected to internet, SCADA systems are vulnerable for cyber-attacks. The recent cyber-attacks push for deploying more secure critical infrastructures.

We also discussed different aspects that we need to consider in designing a more secure SCADA system using a comprehensive model for establishing a framework for securing SCADA systems. Our future works is to study different system modeling methods to improve security to SCADA systems.

REFERENCES

[1] S. Durrani, I. Jattala, J. Farooqi, N. Shakeel and M. Murad, Design and development of wireless RTU and cybersecurity framework for SCADA system, 5th International Conference on Information and Communication Technologies, 2013.

[2] V. Urias, B. Van Leeuwen and B. Richardson, Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed, MILCOM 2012 - IEEE Military Communications Conference, 2012.

[3] H. Piggin, Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security, IET Conference on Control and Automation: Uniting Problems and Solutions, 2013.

[4] S. Amin and X. Litrico, S. Sastry, A. M. Bayen, Cyber Security of Water SCADA Systems—Part I: Analysis and Experimentation of Stealthy Deception Attacks, IEEE Transactions on Control Systems Technology, Vol. 21, Issue: 5, 2013, pp. 1963 – 1970.

[5] S. Amin, X. Litrico, S. Sastry and A. M. Bayen, Cyber Security of Water SCADA Systems-Part II: Attack Detection Using Enhanced Hydrodynamic Models, IEEE Transactions on Control Systems Technology, Vol. 21, Issue: 5, pp. 1679 - 1693, 2013.

[6] G. Dondossola, F. Garrone, G. Proserpio and C. Tornelli, Impact of DER integration on the cyber security of SCADA systems - The Medium Voltage regulation case study, Workshop: Integration of Renewables into the Distribution Grid, 2012.

[7] G. Andersson, P. Mohajerin, M. Vrakopoulou, K. Margellos, J. Lygeros, A. Teixeira, G. Dán, H. Sandberg and K. H. Johansson, Cyber-security of SCADA systems, IEEE PES Innovative Smart Grid Technologies, 2012.

[8] E. I. Gergely and L. Coroiu, H. Maria Silaghi, Dependability Analysis of PLC I/O Systems Used in Critical Industrial Applications, V.E. Balas et al. (Eds.), New Concepts and Applications in Soft Computing, Studies in Computational Intelligence 417, Springer-Verlag Berlin Heidelberg 2013, pp. 201-217.

[9] Stefanov and C.C. Liu, Cyber-power system security in a smart grid environment, IEEE PES Innovative Smart Grid Technologies, 2012.

[10] H. Piggin, Emerging good practice for cyber security of Industrial Control Systems and SCADA, 7th IET International Conference on System Safety, incorporating the Cyber Security Conference, 2012.

[11] S.S Wu, C.C. Liu, A. Stefanov, Distributed specification-based firewalls for power grid substations, IEEE PES Innovative Smart Grid Technologies, Europe, 2014.

[12] T. Cruz, L. Rosa, J. Proença, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, P. Simões, A Cyber security Detection Framework for Supervisory Control and Data Acquisition Systems, IEEE Transactions on Industrial Informatics, Vol.12, Issue: 6, 2016, pp. 2236 - 2246.

[13] Y. Yang, H-Q. Xu, L. Gao, Y-B. Yuan, K. McLaughlin, S. Sezer, Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks, IEEE Transactions on Power Delivery, Vol.32, Issue: 2, 2017, pp. 1068 - 1078.

[14] S. Ghaleb; A. Zhioua; SCADA-SST: a SCADA security testbed, World Congress on Industrial Control Systems Security (WCICSS), 2016.

[15] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono and H. F. Wang, Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems, International Conference on Sustainable Power Generation and Supply, 2012.

[16] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, H. F. Wang, IEEE Transactions on

Power Delivery, Multiattribute SCADA-Specific Intrusion Detection System for Power Networks, Vol. 29, Issue: 3, 2014, pp. 1092 – 1102.

[17] M. Malek, A. Anzalchi and A. Sarwat, A review on cyber security issues and mitigation methods in smart grid systems, SoutheastCon, 2017.

[18] Y. Wang, W. Li, G. Yan and S. Song, Towards a framework for cyber attack impact analysis of electric cyber physical systems, 2017 IEEE International Conference on Industrial Technology (ICIT), 2017.

[19] K. Goutham, P. Mandal and T. Tzu-Liang, Secure SCADA communication network for detecting and preventing cyber-attacks on power systems, Clemson University Power Systems Conference (PSC), 2016.

[20] The Logical Framework Approach (LFA): Handbook for objectives-oriented planning, Norad, Fourth edition, 1999.

[21] GTZ, Methods and Instruments for Project Planning and Implementation, Eschborn, Germany, 1991.

[22] ZOPP: An Introduction to the Method, COMIT Berlin, May 1998.

[23] AGCD, Manuel pour l'application de la «Planification des Interventions Par Objectifs (PIPO)», 2ème Edition, Bruxelles, 1991.

[24] M. N. Lakhoua, Refining the objectives oriented project planning (OOPP) into method of informational analysis by objectives, International Journal of the Physical Sciences, Vol. 6(33), 2011.

[25] M.N. Lakhoua and T. Ben Jouida, Refining the OOPP into Method of Representation of the Information by Objectives, International Transactions on Systems Science and Applications, Vol.7, N° 3/4, 2011.

[26] M. Annabi, PIPO étendue : Méthode Intégrée de Spécification, de Développement et d'Implémentation de Projet (MISDIP), International conference on Sciences and Techniques of Automatic control and computer engineering STA'2003, Sousse, 2003.

[27] E. M. Walter, Introduction à la méthode de Planification des Projets par Objectifs, Rapport de l'atelier de formation REFA, Maroc, 1998.

[28] S. Killich and H. Luczak, Support of Interorganizational Cooperation via TeamUp at Internet-Based Tool for Work Groups, Proceedings of the 6th internationally Scientific Conference, Berchtesgaden, May 22-25, Berlin, 2002.

[29] A. Ghaleb, S. Zhioua, A. Almulhem, SCADA-SST: a SCADA security testbed, World Congress on Industrial Control Systems Security (WCICSS), 2016.

[30] J. Chromik, A. Remke, R. Haverkort, What's under the hood? Improving SCADA security with process awareness, Workshop on Cyber- Physical Security and Resilience in Smart Grids, 2016.

[31] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. AlGhamdi and A.Y. Zomaya, An Efficient Data-Driven Clustering Technique to Detect Attacks in SCADA Systems, IEEE Transactions on Information Forensics and Security, Vol. 11, Issue: 5, 2016.

[32] A. Singh, A. Prasad and Y. Talwar, SCADA security issues and FPGA implementation of AES — A review, 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), 2016.

[33] R. Czechowski, P. Wicher and B. Wiecha, Cyber security in communication of SCADA systems using IEC 61850, Modern Electric Power Systems, 2015.

[34] P. Singh, S. Garg, V. Kumar and Z. Saquib, A testbed for SCADA cyber security and intrusion detection, 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, 2015.

[35] Y. Zhang, L. Wang and Y. Xiang, C.W. Ten, Power System Reliability Evaluation, With SCADA Cybersecurity Considerations, IEEE Transactions on Smart Grid, Vol.6, Issue: 4, 2015.