CYBERSECURITY VULNERABILITIES AND THREATS OF SCADA SYSTEMS IN CRITICAL INFRASTRUCTURES

Vlad Daniel SAVIN [a]*, Costel SERBAN[a]

[a] The Bucharest University of Economic Studies, Romania

ABSTRACT
This paper seeks to analyse the recent exponential growth of the cybersecurity vulnerabilities and threats of SCADA systems in the critical infrastructures. As the critical assets that support the functioning of societies and economies are becoming more automated and IT integrated, the cyber attacks are becoming more susceptible to have potentially disastrous effects. Given the importance of the SCADA systems, successful cyberattacks upon them can have adverse results upon the national economies and societies. Necessary steps are mandatory to be taken in order to improve the cyber protection of the critical infrastructures.

KEYWORDS: *cybersecurity, critical infrastructures, scada systems.*

1. INTRODUCTION

Modern control systems are becoming more complex, digital and inter-connected. The world societies are becoming more dependent on IT systems as we are converging to an information technology economy. The critical infrastructures, following the same path, are becoming more dependent on IT systems (Knowles et al., 2015). In the past, they were isolated from other networks, but today's operators need data to be transferred in real time between industrial and external networks. This created the barrier for malware and hackers to gain access to and disrupt real-time control systems and critical infrastructures. This paper offers an overview of the emerging cyber vulnerabilities and threats and proposes methods and services for combating cyber intrusions.
Supervisory Control and Data Acquisition SCADA represents a system that combines computers networked data communications with graphical user interfaces for complex process supervisory management. These industrial processes are controlled by computers that monitor and control. Historically SCADA systems differed from other industrial control systems ICS by incorporating large-scale processes or including multiple, long-distance factories. The key role of the system is its ability to perform the following key aspects: acquire, communicate, present and control operation over a wide range of other proprietary devices. The security of SCADA and real-time systems is a significant challenge in today's world.
In most cases the SCADA systems contain the following components: a) supervisory computers that collect the data sent from the field devices; b) remote terminal units RTUs and programmable logic controllers PLCs that connect to the sensors and send data to the supervisory computers system; c) communication infrastructure which connects the supervisory computers system with the RTUs and PLCs; d) human-machine interface that presents in a graphical manner the state of the system (Vacca, 2014).
As the world economy is rapidly moving towards an information technology based one so is the landscape of modern national states warfare changing from a physical towards cyber one. The US

* Corresponding author. E-mail address: *vlad.savin@ager.ro*

administration recognized that an important part of its statecraft is made of defensive and offensive cyber operations.
In 2011, one of the most important national led cyberattack took place, which was a joint effort between the US and the Israeli cyber teams. The attack targeted the SCADA system of an Iranian nuclear facility with the intention of disabling the centrifuges of the power plant. In response, the Iranian cyber teams, over a period that lasted more than six months, penetrated the systems of more than forty US financial institutions (Halpern, 2019). It is important to understand the difference of the stakes involved between attacks over financial institutions which might lead to unauthorized permission to financial reports or even worse to a denial of service with attacks over SCADA systems that could have a bigger impact concerning the national institutions given the effects that could result. The business system risks associated with a cyberattack are financial integrity, denial of service and possible loss of information. All these risks could be integrated under the financial and reputation risks. While a SCADA system facing a cyberattack could lose the view of the plant or even more dangerously lose the control of it. The nature of industrial control systems risks being associated with operational and safety. So the potential results of successful cyberattacks over SCADA systems could lead to safety issues and in worst cases to the loss of human lives (Ginter, 2018).

2. VULNERABILITIES AND THREATS OF SCADA SYSTEMS EXPLOITATION

When considering the vulnerabilities of any digital and information technologies we have to analyse how to preserve the confidentiality, integrity and its availability (Goodman, 2007). The nature of the SCADA systems have been drastically changed since their initial design from an isolated network to an open arhitecture which is connected to the outside world. This redesign has led to new opportunities in term of remote access to the previous isolated network but also created some cyber vulnerabilities. As Google offers us the possibility of indexing the web content and returns quickly the searched item there is another engine, which was developed in 2008, very similar to Google, called SHODAN which indexes http headers permitting the hackers to locate computers, servers and thus industrial control systems (Obodoeze & Obiokafor, 2018). Based on SHODAN search engine, the SHINE's project mission was to discover the number of industrial control systems connected directly to the internet. There were discovered more than one million industrial control systems connected to the Internet with their own unique IPs. The cyber security protection of the vast majority of these systems was considered to be weak by hackers. So, all would have to do a hacker would be to determine the IP address of the industrial control system, get a code from Metasploit, which is shared a database of penetration vulnerabilities and then target the attack upon the IP discovered. All this could take place in less than thirty minutes. So, the cyberattacks permits assaults to happen from outside with extreme physical consequences without the need of any physical pressence.
The cyber protection of the SCADA systems is recognized as being weak, given that the systems are robust and were intended to last for long when they were designed initially without the capability of internet connection. Many of the systems are encoded with hardcoded passwords which are known by the hackers and would permit easy access inside. In case of a cyberattack many of these would fail.
Given these risks new security controls should be implemented in industrial control systems to mitigate the weak protection such as firewalls and data diode to segregate the networks from intruders.
As soon as a system had been hacked, the hacker can change the entire operation logic of the system. With Stuxnet, after the malware captured the centrifuges, it changed automatically the logic of the system making the centrifuges to accelerate rapidly. A similar attack could be replicated with even bigger effects. As a defense strategy, some programmable logic controllers may be duplicated

for increase protection, but if the malware is constructed to alter the logic in any programmable logic controller, this defense strategy will not be of any help. The Stuxnet represented the turning point for the regulators for whom became obvious that criminals that attack industrial control systems intend to have physical damages of the plants by altering the logic of the systems.
The number of attacks on industrial control systems is relatively small but the administrators have to be aware of the existing risks and continuously improve the security of their SCADA networks. In any case, integrated security solutions should be taken into consideration for any SCADA system before the process starts operating (Taylor et al., 2013). This might not always be the case and it is vital that the SCADA systems are segregated from the networks that present cyber risks. So, the SCADA system will not be discovered under the SHODAN search engine. The possible key weaknesses of any industrial control system are the software and hardware embedded vulnerabilities and the lack of cyber knowledge of the personnel.

3. EFFECTIVE CYBER DEFFENSIVE STRATEGIES FOR INDUSTRIAL NETWORKS

There is no silver bullet against cyberwarfare attacks (Lonsdale, 2003). The nature of modern digital environments and the need to be connected in real time with the data generated within the SCADA system creates important cyber security challenges. In order to protect SCADA systems from external threats it is important first of all to conduct network assessments, to implement secure firewalls and communication gateways and lastly to integrate data diodes that would separate the industrial control systems from the enterprise and business systems. The data diode would be used as a last resort cybersecurity protection ensuring unidirectional information exchange between the SCADA systems and the business network of the company, effectively eliminating the risks associated with a possible cyberattack.
Another useful cybersecurity solution would be an intrusion detection software (Goldenberg & Wool, 2013) that would trace any malicious traffic within the SCADA system. This tool of detection would notify the system administrators of any intrusion behavior when detected and would possibly block any unauthorized changes in the SCADA system. Furthermore, a forensic readiness plan should be set up in case a cyberattack happens so the investigators would have access to data easily.

4. CONCLUSION

The cyber warfare has seen a rapid development over the last two decades. It is with no surprise that the SCADA systems have been an important target within this new type of warfare. The industrial control systems as are becoming more open in order to meet the requirements of the new information age are also becoming more exposed to cyberattacks that would affect the integrity of these systems. In this paper, we have highlighted the major vulnerabilities and threats that the SCADA systems are facing (Sutton, 2014). We have reviewed one of the most important national led cyberattack with its physical consequences. Based on the results found, we proposed a list of security attributes that have to be implemented in any SCADA system. For further research, it would be useful to analyze for each national critical infrastructure the regulatory protection guidelines defined by the industries and to see if there are any similarities and where to do they differ along with the vulnerabilities and threats given that all the critical infrastructures networks are based on the same kind of industrial control system. The majority of the regulatory guidelines are US based given that they one of the most developed SCADA systems network. It would be interesting to analyze them and see how they could be of any benefit to the European states in terms of setting their guidelines given that the cyber warfare is becoming more popular on the top executives' agendas. Another area of future research would be an analysis of the major incident responses based on the internal forensic reports.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to the entire staff of the PhD Management Department of the The Bucharest University of Economic Studies especially to Professor Ciocoiu for her valuable comments and suggestions, which helped us improve our paper.

REFERENCES:

Ginter, A. (2018). *Secure Operations Technology.* CANADA: Abterra.

Goldenberg, N., Wool, A., (2013). Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *Internatioanl Journal of Critical Infrastructure Protection*, 6(2), 63-75.

Knowles, W., Prince, D., Hutchison, D., Disso, J., Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection,* 9, 52-80

Lonsdale, D.J. (2003). *The Nature of War and Information.* US: Routledge.

Obodoeze, F., Obiokafor, I. (2018). SCADA for National Critical Infrastructures: Review of the Security Threats, Vulnerabilities and Countermeasures. *International Journal of Trend in Scientific Research and Development, 2(2), 974-982.*

Sutton, D. (2014). *Information Risk Management.* UK: BCS Learning and Development.

Taylor, A., Alexander, D., Finch, A., Sutton, D. (2013). *Information security and management principle.* UK: BCS Learning & Development.

Vacca, J. (2014). *Cyber Security and IT Infrastructure Protection.* US: Elsevier.