Supervisory control and data acquisition (SCADA): the security of critical infrastructures nowadays

Mihai APOSTOL, Andreea DINU
National Institute for Research and Development in Informatics - ICI Bucharest
mihai.apostol@ici.ro, andreea.dinu@ici.ro

Abstract: Critical infrastructures have always been the most sensitive, vulnerable area of any system or process. Therefore, no matter how well they are protected, they will always have a degree of vulnerability, as a rule, being the first targets when it comes to destabilizing or even destroying a system or process. In a world where almost all technological processes are based on automation and controlled by industrial control systems (ICS), people rely on these infrastructures directly or indirectly and they have become indispensable to society. Most critical infrastructures are controlled by SCADA (Supervisory Control and Data Acquisition) which means that it comes with flaws, bugs, known and unknown vulnerabilities that can be exploited by any means. The SCADA network is responsible for many functionalities and applications that enable operations at the infrastructure level. SCADA systems are based on an operating flow that starts from collecting information from various measuring instruments and stops displaying information to operators, so that they can act accordingly. Because of this long and important process, SCADA systems are exposed to many cyber threats.

In this article, we will present the main components of SCADA systems and briefly describe their operation and use. Also, we will identify the most common vulnerabilities of control systems and data acquisition and will mention possible types of cyberattack that can target these systems. The effects on the company will be discussed in the event of a successful cyberattack and we will highlight different methods of protection and security in order to prevent or combat any threat.

Keywords: SCADA, vulnerabilities, security, cyberattacks, critical infrastructure, society, threats

INTRODUCTION

Critical infrastructure or critical national infrastructure is a term that generally describes all the resources or systems of a country that ensures the minimum operating functionalities in the governmental, social and economic field. Various government agencies dealing with critical infrastructure security have divided them into two categories. The first category is called commercial infrastructure and includes telecommunications systems, IT and financial services, health system and energy production systems, and the second category is called public infrastructure and contains military services, transportation, government facilities *[Haroun,2018]*.

Supervisory control and data acquisition (SCADA) play an extremely important role in most critical infrastructures. Initially, SCADA systems were built to be operated manually under the supervision of an operator. Nowadays, because the technology has evolved extremely and all the systems have undergone a major expansion, modifications were needed on the SCADA systems in order to be able to access them remotely and to have the ability to measure and collect data over long distances. SCADA networks are the basis of critical infrastructures and include computers and applications responsible for most of the essential functions in providing services and resources. Due to the capabilities of data collection and analysis from control equipment, SCADA systems are very efficient and have a large-scale use. Initially, they were designed to maximize functionality. Therefore, their security is weak, with no emphasis on this aspect. This makes SCADA systems vulnerable to threats such as service interruption and redirection or manipulation of collected data that could lead to public safety issues or the destruction of critical national infrastructure.

In recent years, cyber threats have grown exponentially, with new types of malicious attacks and viruses constantly being discovered. The major interest of cyber criminals seems to be the frequent attack on critical infrastructures, having devastating effects on the countries concerned, in case of success. Due to this fact, the need for SCADA systems to be protected from the possibility of cyberattacks has increased and has become a problem itself. The purpose of the attackers is difficult to detect, as they are of several types from terrorist groups, which have a well-defined purpose to simple people who are just exploring, not knowing exactly what advantage they will gain. Security experts try every day to find new security solutions, as efficient and with a greater coverage area in the threats that float in the cyber space. They try as much as possible to make known the various cyber-attacks or dangers they have faced and offer the best solutions to combat them.

Following the article, we will present the main components, functionalities and use cases of the SCADA system. We will discuss the threats and dangers to which the SCADA system is subjected in cyber space. Also, there will be illustrated two real cases of cyber-attack on SCADA systems, analyzing the causes and effects resulting from malicious actions. In the end, possible security solutions will be highlighted in order to raise awareness of the importance of protecting any system, especially the systems that coordinate the critical infrastructures of a country.

ABOUT SCADA

SCADA (Supervisory Control and Data Acquisition) is an industrial control system that monitors and controls industrial processes like manufacturing, traffic signals, recycling and many others. It is also widely used in critical infrastructure like water treatment, public health, telecommunication, mass transit, electric power generation, nuclear power plant, banking and many other infrastructures that are necessary for the society. SCADA manages subsystems that are geographically distributed over large areas, sometimes hundreds of square kilometres. SCADA refers to the combination of telemetry and data acquisition that gathers process information which are transmitted to the central computer, via a communication system, where necessary analysis and control are taking place (Gordon, 2004). These system transfers data between a central host computer and one or more PLC (Programmable Logic Controllers) or/and RTU (Remote Terminal Unit). SCADA systems collect information, sends the information to a central computer, sends event information such as alarms (and also information about the event like critical alarm level) and displays the information in a human readable form and it can be controlled locally or remotely by an human operator (Knapp, 2015).

A typical SCADA system, as illustrated in ***Fig. 1***, is constructed of two major elements. The first element is the physical one, being represented by many field devices, and the second element is the software part, which manages and controls all the equipment.

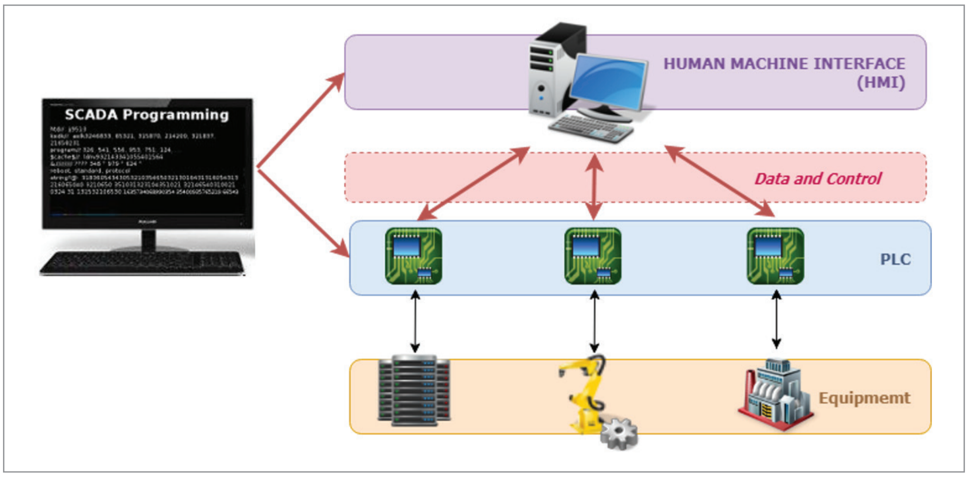

Fig. 1: *Typical SCADA system (https://www.dpstele.com/scada/programming-concepts.php)*

A. FIELD DEVICES

Field devices are extremely important in a SCADA system. They generally deal with the measurement and collection of data over very long distances. One of the main components of the SCADA system is programmable logic controller (PLC). A programmable logic controller is an electronic device that is controlled by a microprocessor and reads input signals from sensors, sends output signals based on the processed input signal to field devices and execute supervisory control tasks. Unlike desktop computers, PLC devices were built to withstand unfriendly environment conditions such as high temperature, humidity, electromagnetic fields, vibrations and other conditions. They usually operate without any down time and can be deployed for 10–15 years and sometimes longer *[Edward, 2016]*. A PLC has a CPU, communication interface, I/O modules that can be either analog or digital and a power supply. It operates an RTOS (real-time operating system), has a control loop, it uses ladder logic and the read/write/execution time of a PLC is very short, down to a few milliseconds. Also, the intelligent electronic device (IED) is a crucial component of SCADA system architecture. An intelligent electronic device is a device that incorporates one or more processors having the ability to send and receive control data from. It has more capabilities than a PLC, functions like protection, control, monitoring and it communicates independently without any aid from other devices *[Edward, 2016; Gordon, 2004]*. Another pair of very important devices are remote terminal unit (RTU) and master terminal unit (MTU). A remote terminal unit act as a slave device in SCADA systems. An RTU is the same as an PLC but with a few differences. It is more suitable for wireless communication and does not support control algorithms and control loops. Due to today's technologies, cheaper hardware and standardization, RTU and PLC functionality are overlapping *[Knapp, 2015]*. Master terminal unit is the central controller and it can be a server or a group of servers. In most cases, the Human-Machine Interface (HMI) is usually installed on the MTU and the software applications used to program PLC/RTU/IED devices. The MTU communicates (send and receive data) with low-level devices, displays the information received from PLC or RTU in a readable form like charts, graph or text and perform acquisition. The MTU can monitor and control the entire SCADA system *[Shahzad, 2014]*.

B. SOFTWARE COMPONENTS

Like any hardware device in a system, they require software support to be able to communicate with each other, to be controlled by SCADA system operators, etc. The human machine interface (HMI) is one of the most important assets in a SCADA system. It is a software application which can provide real time up to date information about the industrial process. HMI allows an operator to control, configure and troubleshoot the plant assets, provides data conversion, interface between hardware and software communication and displays all SCADA operational information and communication status between devices *[Edward, 2016; Shahzad, 2014]*. Everything that the HMI displays is storing in historians. The Historian is a database server where all process information of all types is stored. Usually, this is very useful when are required analytics, management, optimization, report generation and much more. All the physical components communicate with each other through industrial network protocols. A network protocol is a set of rules needed in order to transmit information through a communication channel. An industrial network protocol is a real-time network protocol developed to interconnect ICS assets. Most of them were built to support RS-232/422/485 interface. The most popular protocols are Modbus, DNP3, OPC, Profibus and ICCP.

The architecture of a SCADA system is quite elaborate, the equipment being distributed on the ground over a very long distance. Both hardware and software are exposed daily to threats and sabotage hazards. Also, the SCADA system by nature of construction presents various vulnerabilities that can be exploited by people with malicious intentions.

VULNERABILITIES AND THREATS OF SCADA

SCADA system components were not built with security in mind, they were developed to deliver high performance, safety, reliability and withstand harsh environment. Most of today's SCADA systems are old and uses proprietary software, hardware and communication protocols which includes error detection and correction but does not include secure communication. SCADA systems were limited in communicating with outside sources, as they were often isolated from external networks. Now, SCADA systems are connected to other networks which brings more insecurity.

Searching and finding vulnerabilities in SCADA systems is not an easy task. Known vulnerabilities may not occur in every SCADA system because every SCADA system has some unique characteristics and features. All SCADA systems have physical vulnerabilities despite that some components are built to withstand physical damage. Unauthorized employees having physical access to SCADA assets represents a high risk; Access of personnel should be restricted to those who are necessary. Access to SCADA devices by unauthorized personnel can lead to physical damage/ destruction of hardware, stolen hardware and data, unauthorized use of removable media. A power failure can happen any time. If a power shortage occurs and no backup power is present, the system will shut down and after powering the system, some settings may restore themselves to the default settings which in most cases, these settings are totally not recommended. Leaving unsecured ports open, as USB and RS, can lead to connection of untrusted devices and installation of malicious software (key loggers).

Incorporating security into SCADA architecture and design must start with budget and schedule of the system. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms *[Keith, 2015]*. If the system does not have a security perimeter defined, it is not possible to ensure that the necessary security controls are deployed and configured properly; this can lead to unauthorized access to systems and data and other problems (Keith, 2015). The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within portions of the infrastructure. Without remediation, these gaps may represent backdoors into the ICS.

Policies and procedures are some of the most important aspects in a SCADA system as most of the attackers rely on untrained personnel because they can reveal critical information if no suitable security/awareness training program exists and no security policy has been deployed or there are insufficient security documentation. More risk consists in the absence of audits regarding security or they are performed rarely, manuals and implementation guides are incomplete or absent and some of them are mandatory in order to perform some audits. An inadequate incident and response plan can lead to many problems regarding recovery after an attack. Incident detection and response plan are required in order to quickly detect incidents, minimize damage, and mitigate exploited vulnerabilities and preserving data for later forensic investigation. In case of danger, an emergency plan/disaster recovery must exist (other than those required by law) and it must be very well developed and tested. If a dangerous event occurs and no such plan exists, it could jeopardise the entire company or in the worst case, it can lead to loss of human lives.

Operating system (OS) and software patches may not be developed until significant vulnerabilities are found or vendor declines to develop a patch, searching for vulnerabilities implies expensive and time consuming assets testing; even more, the elapsed time for such testing and subsequent distribution of updated software provides a long window of vulnerability. Many today's SCADA systems uses OS that have reached EOL (end-of-life), hence they are no longer maintained and patched. The organization doesn't know what kind of devices it has, where they are located, what versions it has or patch status is, delivering an inconsistent and ineffective defence stance. A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure SCADA is protected against inadequate or improper modifications before, during, and after system implementation. A lack of configuration change management procedures can lead to security oversights, exposures, and risks. To properly secure an ICS, there should be an accurate listing of the assets in the system and their current configurations. These procedures are critical to executing business continuity and disaster recovery plans *[Keith, 2015]*. Using improper configurations can lead to a series of problems. Poor configuration can leave useless function consuming resources, unnecessary protocols and ports open that may contain known or unknown vulnerabilities. Leaving sensitive data in plain text, unencrypted, can compromise the security system. If data is stored on portable devices and these devices are stolen, it brings more vulnerabilities in the system. A common attack is installation of malicious software (virus, Trojan, worms, ransom ware etc.). An antivirus software should be present in any ICS and kept updated. Outdated antivirus software can leave the system vulnerable to new malware. Also implementing an anti-malware software without rigorous testing can disturb SCADA processes.

If no firewall present or inadequate configuration of the firewall allows unnecessary/unwanted data to travel between networks. Malicious software can spread this way and may allow an attacker to sniff data packets which can lead to unauthorized system access. Using Unsecure communication protocol may lead to numerous consequences: Most industrial communication protocol does not have security measures. A protocol without authentication allows an attacker to modify, reply and spoof data or devices. One of the SCADA requirements is data integrity; Most protocols do not offer integrity protection which can allow undetected manipulation of communications. Also, there are protocols that send data in plain text (HTTP, NFS, FTP) so an attacker can easily use a packet analyser to decode information *[Keith, 2015]*. Wireless networks are one of the easiest network types to hack. Authentication is needed between access points and clients in order to avoid rogue access points and to avoid an attacker connecting to a SCADA wireless network. One aspect it should not be overlooked is data flow control; In order to prevent data access and illegal operations, data flow control is needed to restrict which information is allowed between systems *[Jason, 2003]*.

Ladder logic is used in all PLC programming and it is based on graphical objects that represents a circuit diagram. An example of such programming language is the Logo! Soft Comfort for Siemens PLC which provides basic functions

(OR, XOR, NOT, AND, NAND) and special functions (delay, timer, alarm, counter and more). By gaining access to ladder logic, an attacker can modify the PLC program which can lead to hazardous impact on critical infrastructures and produce unpredictable results. Inadequate privileges allow unskilled employees having access to programming software and configuration options could lead to unwanted modifications and device corruption. Data validation is a known problem not only to ICS; If user input or received data is not properly validated, it could drastically increase the vulnerabilities, allowing SQL injection, buffer overflows, XSS and many more. Some software setting and options may or may not be enabled by default and due to poor training or employees are not even aware of them, making the software useless to some extent (Keith, 2015). A dangerous vulnerability is the Zero-day; It is an unknown vulnerability and no patch is available in order to mitigate it. If an attacker discovers such a vulnerability, he can exploit it for some time until the system vendor learns about the vulnerability and develop a patch.

All these vulnerabilities existing in the SCADA system have determined the cybercriminals to develop many types of attacks, exploiting every weakness of the system. A very well-known type of attack is phishing. It is a type of attack where an attacker attempt to steal sensitive information like credit card details or login credentials by communicating to the target, making them believe they are communicating with a trustworthy entity. Also, a big threat for SCADA system is the infection with a malware. A malware is a malicious software developed with the purpose of causing damage. It includes worms, viruses, spyware, Trojan, ransom ware and more. These malwares can reach a network by accessing email attachments, clicking malicious link, downloading from untrusted web sites, installing risky software or by connecting compromising external devices. These malware installs without any notification and most of them operate without user knowing except ransom ware which can be immediately noticed because it encrypts the files demands payment in exchange for file decryption. Malware of all kinds can cause a lot of damage, especially in the industrial network. Another way that the cybercriminals steal information is by man-in-the-middle attack. It is an attack where an attacker positions himself between two entities having the objective to alter the communication taking place. Performing this technique, the attacker can obtain personal information, credit card number or login credentials.

These were just a few of the existing examples of attack types. Over time, these types of attacks have been used countless times on control systems, especially systems that control critical infrastructures. When these were successfully completed, the damage was major, leaving traces in all areas of a country's development.

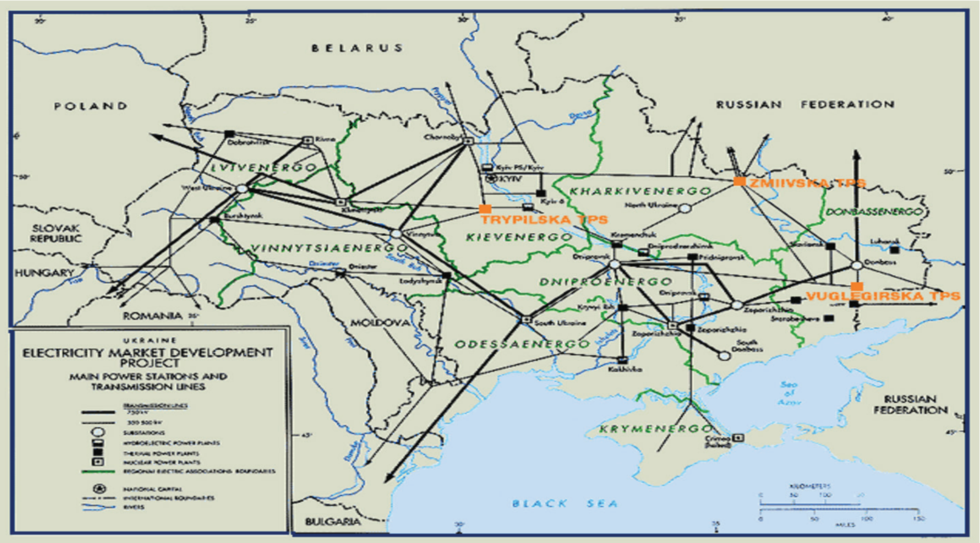

***Fig. 2:** Map of Ukrainian Electricity Grid (https://www.geni.org/globalenergy/library/national_energy_grid/ukraine/ukrainiannational electricitygrid.shtml)*

EFFECTS OF A SUCCESSFUL CYBERATTACK

Successful attacks, especially cyber-attacks, on a critical national infrastructure would have devastating effects for the entire population of that country. Sometimes, even a simple interruption of a service can causes a great deal of economic, social or governmental damage. Here are some examples, in which the attacks were successful and caused harm to the victims.

A. UKRAINIAN POWER GRID ATTACK

On December 23, 2015 the IvanoFrankivsk region of Ukraine remained without electricity for about 6 hours. This incident was found to be a cyber-attack on three electricity suppliers, carried out by Russia, according to Ukraine.

According to the investigation following the incident, a few months before it was sent an email to the employees of three large electricity suppliers in Ukraine. The email turned out to be malicious, activated macros in an attached Word file. This led to the installation of a malware program called BlackEnergy3. BlackEnergy3 is a Trojan that is generally used to conduct DDoS attacks. It is known that since 2014 a group called "Sandworms" has developed this malware for SCADA systems. After installing the malware, the attackers monitored the network and thus managed to obtain the credentials of one of the employers for connecting to the company system. Since then, the attackers have gone through several stages to cause damage. The first step consisted in deactivating the power supplies that provided backup power for the control systems. Then the attackers used access to SCADA systems to open the switches and overwrite the firmware, preventing further control of the switches. The last step was to use a program called "Kill Disk" to overwrite the computers in the control center, restricting the access of any operator that could act. Even though the attack time was only six hours, about 225,000 customers suffered. Although the attackers only wanted to send a message, without causing major damage, the threat of destruction of the electrical system existed. Ukraine claims the attackers were from Russia, but Russia never took responsibility for the incident *[Zetter, 2016]*.

B. STUXNET

Stuxnet is a cyber-worm that was first discovered in 2010, being responsible for attacking more than 50 facilities in Iran, especially the nuclear facility. It operates in three stages. The first step consists in targeting some computing machines that have installed a Windows operating system. After infiltration, the worm begins to replicate continuously.

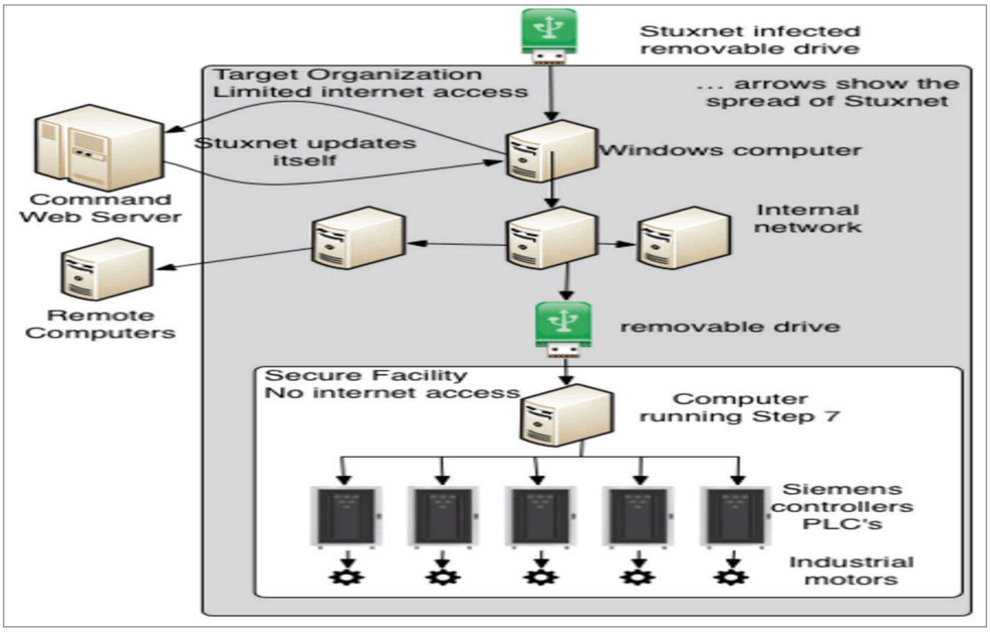

Fig. 3: *How Stuxnet spread (https://www.researchgate.net/figure/How-Stuxnet-Spreads_fig1_269326779)*

The second stage is the infiltration of the software Siemens Step7, widely used in the network industry that operates critical infrastructures. In the final stage, the worm already has access to the main components of the control systems and begins to act maliciously. It is known that this cyber worm infects a system in general through a USB, being able to spread in all other programs of the system *[Holloway, 2015]*.

Stuxnet was merely a weapon of the United States and Israel to destroy or at least delay the Iranian nuclear weapons development program. They believed that if Iran were able to complete the construction of nuclear weapons, they would launch an attack on Israel that would lead to a regional war. Cyber worm was never intended to spread, its main purpose being to infect systems that controlled nuclear activity. Many Americans have claimed that infecting other facility systems, other than the nuclear one, was an action backed by Israel, by changing the source code of the virus *[Fruhlinger, 2017]*.

The launch of the Stuxnet virus and the success of the attack on Iran's nuclear network had major effects nationally, but also internationally.

At the national political level, the virus has discredited the Iranian government for not having the necessary capabilities to defend the country's nuclear facilities from such a cyber-attack. At the same time, being an unprecedented case at that time, Iran did not know how it was supposed to react following the attack, not knowing the guilt for the incident. Fortunately, there were no human losses. The fact that the virus has spread to other computers in the world and not only harmed the control systems of the nuclear network, has created a feeling of uncertainty and fear globally *[Baezner & Robin, 2017, p9]*.

In the technological field, Stuxnet aimed directly at causing damage to centrifuges from the nuclear plant in Natanz. It is known that the virus had the ability to affect the speed of operation of the centrifuges by alternating it from high speeds to low speeds, which causes wear among them. Thus, uranium production decreased considerably during infection. This cyber-worm has directly affected the major providers of operating systems and specialized equipment. After it was found out that the nuclear installation system was infected, providers like Microsoft and Siemens developed patches and updates to protect working tools from this type of virus. As another harmful consequence of the virus, it can be mentioned that among the operators the distrust has been installed, any malfunction being suspected as a result of a possible cyber-attack. Economically, Iran suffered a great deal because during the infection it was necessary to change 1000 centrifuges. This was not a very easy action because Iran does not have access to international markets for the purchase of nuclear materials. They had to build their own centrifuges, which had a major impact on the budget and stock of materials. *[Baezner & Robin, 2017, p10]*.

At the international level, the cyber-attack has managed to slow down the process of building Iran's nuclear weapons, which has relaxed the atmosphere between Iran and Israel. Israel's position has changed with the realization that there will be no need for a direct air strike on their part to damage Iran's enrichment with uranium deposits *[Baezner & Robin, 2017, p11]*.

From a more positive perspective, the discovery of the Stuxnet virus represented the awareness of the cyber dangers that exist today. Thus, it has been found that although most critical infrastructure control systems are not connected to the internet, this is no longer a safe way of protection. Since the Stuxnet incident, the security specialists of the major providers of control systems and specialized equipment have investigated their vulnerabilities and tried to eliminate them or at least find solutions for their protection. This has led to the massive development of technologies designed to ensure security.

POSSIBLE SOLUTIONS TO THE SECURITY PROBLEM

Most incidents in SCADA systems are related to human error resulted from social engineering or employees. One of the main human weakness is curiosity. Someone who found a removable device is likely to take it and connect it to a computer just to see what it contains, and it can contain dangerous malwares. In order to avoid unwanted removable devices connected to the SCADA system, USB auto play should be disabled, and free USB ports disabled as well (until new devices need to be connected). All SCADA removable media and devices must provide some procedures in order to properly destroy these assets (formatting will only delete the file table, data remaining).

Social engineering is a powerful "hacking tool" and it is based on psychological manipulation, driving employees to disclose information or perform malicious actions. Training of staff is mandatory in order to avoid such events and employees should demonstrate their competence at hiring and after any kind of training program. They need to know the details that makes the difference between a real and a fake email. Employees can also be tricked by SMS or phone call by someone who is pretending to be a legitimate employee, or someone shows up at a site pretending he must make food delivery, or he is here for equipment maintenance. This kind of problems can be mitigated by a well-defined security policy and restricting user privileges to only those required.

A common problem is that users can operate terminals having more permissions that necessary. Also, similar problems appear in some software applications running with admin/root privileges by default. Restricting user privileges to only those required and lowering software permission will decrease the user access to critical assets.

An incident detection and response plan will greatly increase security and optimize network traffic as it can detect unnecessary/unwanted network traffic if the incident detection and prevention system is correctly deployed and configured.

Periodic audits should be performed to ensure quality and to determine if the system is performing as intended. IT audits usually focus on recordkeeping, but some SCADA devices operates years without any downtime so they cannot provide the needed audit records *[Keith, 2015]*.

Passwords should have a balanced complexity and length. A long and complex password may sometimes represent a problem; In a critical scenario were human intervention is needed, under the pressure of danger, one could have problems in recalling the password or incorrect password inputted and locked account because of a wrong password entries limit. Passwords should not contain predictable sequence of symbols, common words and numbers and must not be found in dictionaries (attackers can use rainbow tables).

Physical authentication could provide an increase in security. Access cards can be an effective form or authentication for computer access and can be configured to enable/disable control actions, but access cards can be lost or borrowed. Another method could be authentication by biometrics will increase security, especially if it is used as the second factor authentication. Computers, laptops and other SCADA assets used for PLC programming should never leave the site.

Encryption can be used for additional security on data, but it consumes resources in order to authenticate/encrypt/decrypt and can introduces some issues like key management. Considering this communication latency, use of encryption should be carefully weighted if is an appropriate solution.

VPN (Virtual private networks) are widely used in ICS and SCADA systems as they provide protection and secure access from untrusted networks. The most common VPN technologies are Secure Sockets Layer (SSL), Secure Shell (SSH) and Internet Protocol Security (IPsec).

Any ICS or SCADA system must have an antivirus solution correctly configured, updated and 24/7 uptime in order to be fully effective. It can be deployed on servers, mobile devices or firewalls.

Patching OS and OS components will reduce SCADA vulnerabilities but, in some cases, these patches bring problems, increase risk and expose to other vulnerabilities. Because many SCADA systems uses old OS that reached EOL, patching is not applicable.

CONCLUSION

Managing SCADA systems can become a challenge nowadays, if we do not consider the security measures necessary to protect it from any danger. Unfortunately, many SCADA network systems are still old, outdated, unmonitored and unprotected, being the sure target of cyber-attacks but replacing, upgrading old system assets and moving to newer software components will boost cyber security. Given the evolution of technology today and all the dangers that threaten the critical infrastructure of a country, it is essential that control system operators and those who use and produce these systems are aware of the importance of their security. Attacks on SCADA systems are both physical and cyber, and it is compulsory to align safety measures accordingly.

Each SCADA system has its own sensitivities and it is necessary to analyze these vulnerabilities and take protective measures. Successful attacks on the critical national infrastructures of a country, destroy the economy and peace of a country, some incidents ending even with major losses of human lives.

ACKNOWLEDGEMENT

This research was supported by Romanian Ministry of Research, project number 3N/2019.

REFERENCE LIST

A, Shahzad, Musa, S., Aborujilah, A. and Irfan M. (2014), THE SCADA REVIEW: SYSTEM COMPONENTS, ARCHITECTURE, PROTOCOLS AND FUTURE SECURITY TRENDS, Windfield College, Kuala Lumpur, Malaysia, available at https://pdfs.semanticscholar.org/c242/2bb77503c0b4daf54e1859f3268dde0bef72.pdf , accessed on 12nd January 2020.

Alfarsi, Haroun (2018), Critical Infrastructure: Definition and Examples, available at https://www.profolus.com/topics/critical-infrastructure-definition-and-examples/ , accessed on 14th January 2020

Baezner, Marie and Robin, Patrice (2017), CSS CYBER DEFENSE PROJECT Hotspot Analysis : Stuxnet, available at https://www.researchgate.net/publication/323199431_Stuxnet , accessed on 16th January 2020

Colbert, Edward J.M. and Kott, Alexander (2016), Cyber-security of SCADA and Other Industrial Control Systems, Fairfax, USA, Springer, ISBN 978-3-319-32125-7

Fruhlinger, Josh (2017) What is Stuxnet, who created it and how does it work?, available at https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html , accessed on 16th January 2020

Gordon, Clarke and Deon, Reynders (2004), Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, Oxford, Burlington, Elsevier, ISBN 07506 7995

Holloway, Michael (2015) Stuxnet Worm Attack on Iranian Nuclear Facilities, available at http://large.stanford.edu/courses/2015/ph241/holloway1/ , accessed on 15th January 2020

Knapp, Eric D. and Langill, Joel Thomas (2015), Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems, Waltham, USA, Elsevier, ISBN: 978-0-12-420114-9

Sidney E. Valentine Jr. (2013), PLC Code Vulnerabilities Through SCADA Systems, University of South Carolina, available at https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1804&context=etd, accessed on 19th January 2020

Stamp, Jason, Dillinger, John, Young, William and DePoy, Jennifer (2003). Common Vulnerabilities in Critical Infrastructure Control Systems, Sandia National Laboratories, USA, available at https://www.smartgrid.gov/files/Common_Vulnerabilities_in_Critical_Infrastructure_Control_Sy_200310.pdf , accessed on 15th January 2020

Stouffer, Keith, Pillitteri, Victoria, Lightman, Suzanne, Abrams, Marshall and Hahn, Adam (2015), Guide to Industrial Control Systems (ICS) Security, NIST, Gaithersburg, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf , accessed on 14th January 2020

Zetter, Kim (2016), Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, available at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ , accessed on 14th January 2020