ICS in the HPP Perucica as a national critical infrastructure

Ana Grbovic, HPP Perucica, EPCG

Abstract: Because of the frequent examples of sophisticated cyber attacks, such as Stuxnet, Night Dragon and Duqu, it is necessary to implement new security measures in the ICS systems. The paper discusses about the importance of defining ICS as a critical national infrastructure. Security concepts take into account the specific requirements of process control which in general differ significantly from the requirements of Corporate IT. Also, paper describes the concept of deep hierarchy security known as "defense in depth" on the existing system, as well as the possibility of extending and improving the security of ICS (Industrial Control System) and SCADA (Supervisory Control and Data Acquisition) system at HPP Perucica.

***Key words* — critical infrastructure, ICS, SCADA, cyber security, defense-in-depth**

I. INTRODUCTION

Industrial process control systems (ICS) are control and monitoring networks and systems specially designed to support industrial processes. These systems are responsible for monitoring and managing the various processes and operations, such as the distribution of electricity and gas, water treatment, oil refining or rail transport. The largest subgroup of ICS is a SCADA (Eng. Supervisory Control And Data Acquisition), platform that is used in the HPP "Perucica" to control and monitor industrial processes - from simple commands on production units up to the incredibly complex operations associated with protective functions.

In recent years, ICS has gone through a significant transformation from proprietary, isolated systems to open architecture and standard technologies highly interconnected with other corporate networks and the Internet. All this has led to a reduction in costs, ease of use and the possibility of remote control and monitoring from different locations. However, an important drawback derived from the connection to the Internet and open communication networks has increased the sensitivity of computer networks to attacks [1].

SCADA systems' traditional role is changing as the Industrial Internet of Things (IIoT) continues to take a larger role. SCADA systems were not originally designed for cyber security and plants need to adjust to this new reality. With the development of information systems there is a need for exchange of information between the Process and Corporate information systems, as well as the distribution of data from Process systems to the global internet network, which provides access to a wide range of applications.

ICS systems have roots in proprietary technology that was traditionally isolated from the enterprise information technology (IT) infrastructure. These platforms were not originally designed for cyber security [2].

Industrial process control systems represent a strategic asset against the growing number of catastrophic terrorist attacks that affect critical infrastructure. In the last decade, these systems are faced with a significant number of incidents, including Stuxnet, which has created a lot of concern and discussion among all actors involved in this field.

There are many different causes of incidents at ICS, such as random error of an administrative nature or errors that occur during the system updates, insider attacks and weaknesses. Risks of industrial sabotage or attack under the sponsorship of people whose aim is disruption of critical infrastructure are the most dangereous. These types of threats can have potentially devastating outcomes if they execute successfully. To protect the SCADA system, it is essential to evaluate the risk of its exposure to attacks and implement all necessary security measures.

II. ICS SAFETY IN NUMBERS

A. *Frequency of the ICS systems*

The ICS components available from the Internet (shown on Figure 1) are concentrated in the European region (41.41%) despite the modest numbers in individual countries. South America lags behind the Old World (37.46%), Asia holds the third place (12.39%).

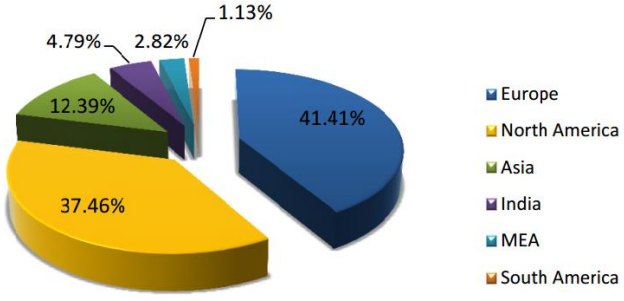

Figure 1. ICS Allocation by Regions

Almost the third part of the ICS systems, which elements can be accessed from the Internet, are located in

Ana Grbović, EPCG, 8 mart br. 76, 81000 Podgorica, Crna Gora (telefon: 382-69-061342; e-mail: ana.grbovic@epcg.com).

the USA (31.3%). Italy follows far behind (6.8%), South Korea rounds out the top three (6.2%). Russia holds the 12th place with 2.3%, and only 1.1% of ICS systems available from the global network are located in China [3].

B. Types of ICS Systems

Most often the global network contains various SCADA components including HMI. They account for 70% of all detected objects. Another 27% of the ICS components are programmable logic controllers. Various network devices used in ICS networks (referred to as the Hardware in the following chart) were detected in 3% of cases [3].

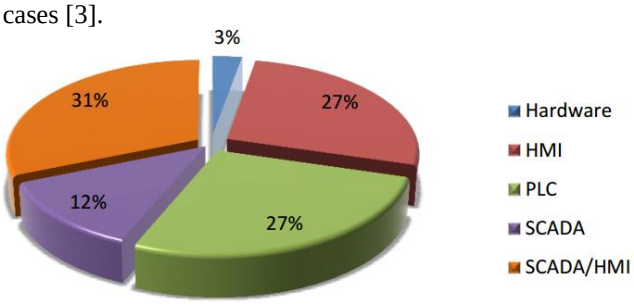

Figure 2. ICS Components

C. Vunerabilities of ICS systems

The report chart below indicates that 90% of the examined ICS vulnerabilities occurred from 2011-2015. Since Stuxnet was publicly disclosed in mid-2010, it could have triggered increased interest in discovering control system vulnerabilities and exploits. Also, between 2014 and 2015 there is a 49% increase [4].

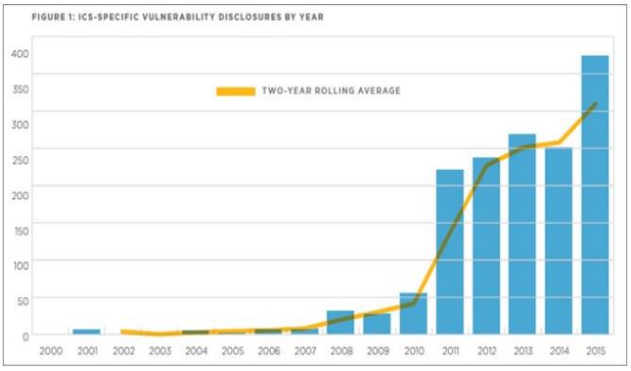

Figure 3. ICS specific vulnerability disclosures by year

Stuxnet is the first virus that was created to attack critical infrastructure of power plants and electrical networks. It is an incredibly sophisticated malware that has a clearly defined target. If, for example, it appeared on a computer, no damage will be made, unless the PC is not connected to the SCADA system specific [5].

III. CRITICAL REVIEW OF THE CURRENT ICS SECURITY POLICY AND PRACTICE AS A NATIONAL CRITICAL INFRASTRUCTURE

The key documents on cyber security in Montenegro are: Study with defined competences of state bodies in combating cyber crime (adopted in 2012), Cyber security strategy of Montenegro (adopted in 2013) for the period 2013-2017, Methodology for critical infrastruture selection (adopted in 2014) and annual reports on incident situations on Internet.

The key part of the legislation is the Law on Cyber Security (Official Gazette of Montenegro, nb. 14/10).

The analysis of the current situation in Montenegro shows that critical infrastructure is not officially defined. For the purpose of forming the National CIRT Team, Ministry for Information Society and Telecommunications, in cooperation with the Company IMPACT in Malaysia, made a review of the critical sectors in Montenegro based on the recommendations of international criteria. This recommendations recognize the energy sector as a national critical infrastructure.

The positive side of Cyber Security Strategy from 2013 is that it supports promotion and implemantation of cyber security measures. However, emphasis is given to IT cyber security development, mainly realized through different government sectors. Insufficient attention is paid to the potential security of ICS systems with its propriatery protocols.

On the other hand, the Cyber Security Strategy represents a certain step forward when it comes to the application of the principles of sustainable development, in comparison to earlier situation.

Key priorities defined in the Cyber Security Strategy are to set the vision, scope, objectives and priorities, monitor the risk assessment at the national level, take into account existing policies, regulations and capacities, develop the clear management structure, identify and engage stakeholders, establish the mechanisms for the exchange of confidential information, develop of cyber-security contingency plans, organize the cyber security exercises, establish public-private partnerships establish the basic safety requirements, establish mechanisms for incidents reporting, increase public awareness about this issue, engage in international cooperation to harmonize national strategy on cyber security [6].

One of the problems is the lack of the necessary skills for a successful defense of incidents, as well as need for changes and amendments or enactment of new legislation, on the basis of which it would be possible to successfully detect and prosecute persons involved in all forms computer crime.

Also, it is noticed that any kind of examination of incidents on ICS has never be done since annual reports on incident situation does not treat it at all.

After all, development and planning of the national cyber crisis plan is an important factor in the overall planning of the state cyber security. It should be realistic and accurate but also it should take into account all possible participants. This involves the interaction of public and private sector.

An important part of this process is the identification and definition of critical national infrastructure, threats and risks connected to it.

IV. IMPLEMENTED SECURITY MEASURES AT HPP PERUĆICA

To limit the exposure to cyber attacks, networks and devices with SCADA protocols, are isolated from other networks (Figure 4). These components are not linked to the Internet. Access to the other networks is strictly regulated by limiting the input / output traffic on strictly necessary protocols.

network SCADA showed how well these links are protected. Following types of connections were identified and estimated:

- Internal LAN and WAN, including business networks
- Internet
- Wireless network equipment, including satellite uplinks
- Relationship with business partners, suppliers and regulatory agencies

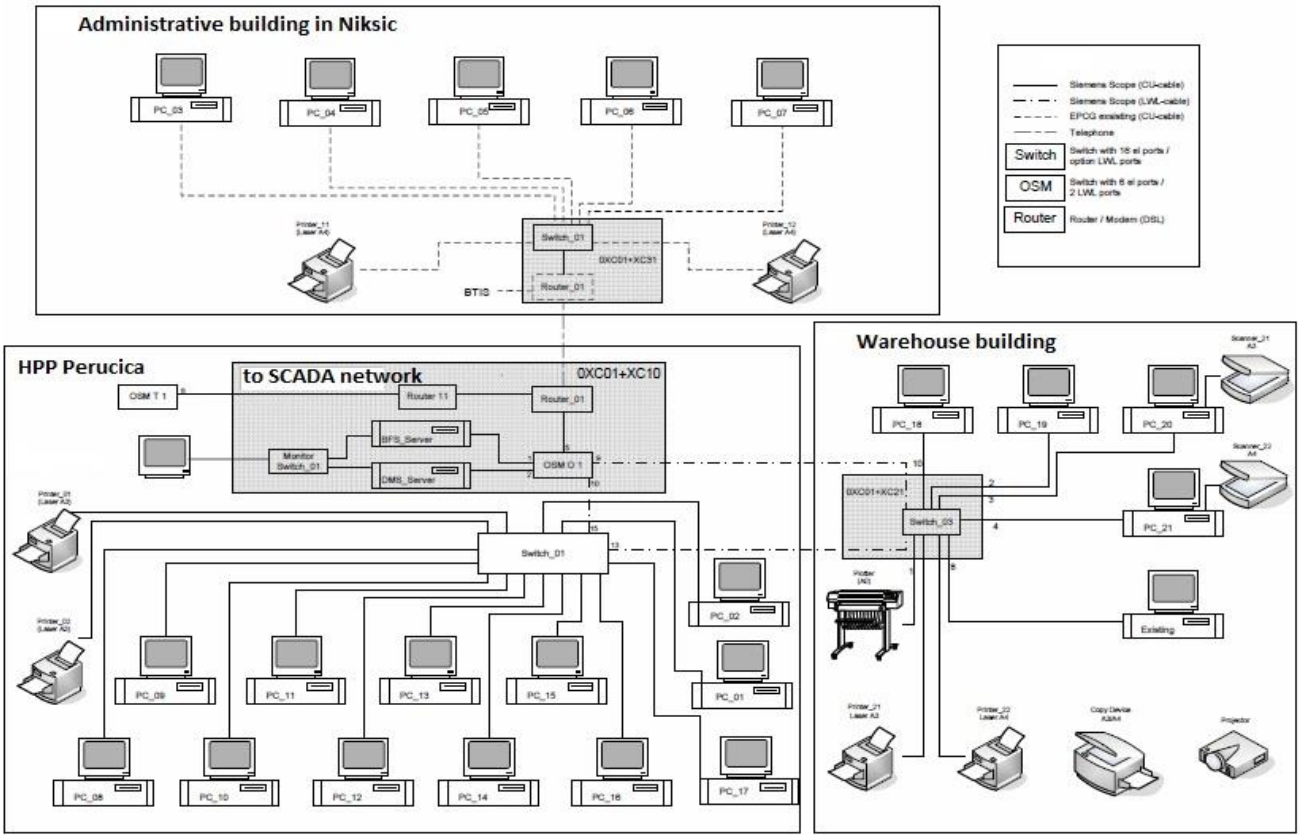

Figure 4. Connection of SCADA network from HPP Perucica with other networks in the company

The following steps represent the activities carried out in the implementation phase of the project, in order to establish an effective cyber security program:

A. Network protection strategy based on the principle of defense-in-depth

The basic principle, which is a part of a network protection strategy, is the principle of defence-in-depth. Defense-in-depth takes into account design stage of the development process, and it is an integral part of all technical considerations and decisions relating to the network. Single points of failure are eliminated, while the cyber defense is layered in order to limit and reduce the impact of any security incidents. In addition, the system is protected by the second system in the same layer [7].

B. Identification of all connections with the SCADA network

A thorough analysis of the risk assessment indicated the necessity of any connection to the SCADA network. A comprehensive understanding of all connections to the

C. Turning off all unnecessary connections to SCADA network

To ensure the highest level of SCADA system security, it is necessary to isolate the SCADA network from other networks to the greatest possible extent. Any connection to another network introduces security risks, especially if the relationship creates a route to the Internet. Although a direct link with other networks can provide an efficient exchange of information, insecure connections are simply not worth the risk.

D. Evaluation and strengthening of the security of all remaining connections to the network SCADA

In order to valuate the level of protection, testing and vulnerability analysis was conducted on all remaining connections to the SCADA network. This information, together with the risks from the process, was used in developing a strong strategy for the protection of all connections to the SCADA network. As the SCADA network is secure as the its weakest connection point,

firewalls and other appropriate security measures have been implemented at every entry point.

E. Strengthening SCADA network by removing or disabling unnecessary services

SCADA servers that use commercial or open source operating systems can be exposed to various attacks through standard network services. Removing or turning off unused services and networks, like a demon, reduce the risk of direct attack which is especially important when the SCADA network is connected with other networks.

F. Place strict controls over any medium that is used in SCADA network

Modem, wireless, and wire networks used for communication and maintenance represent a significant vulnerability of SCADA networks. A successful attack could allow an attacker to bypass all other controls and to have direct access to SCADA resources. To reduce the risk of such attacks, such incoming access IS disabled and has replaced by the VPN system [8].

V. MEASURES THAT SHOULD BE IMPLEMENTED TO INCREASE SECURITY OF SCADA NETWORK

A. Do not rely on proprietary protocols and factory settings security

Some SCADA systems use a unique, proprietary protocols for communication between the device and the server from the field. Often the security of SCADA system based solely on the confidentiality of these protocols. Unfortunately, unclear protocols provide very little "real" security. For this reason, you should avoid proprietary protocols and factory settings, it is necessary need to check whether manufacturers present interfaces allow the safe functionality of the system.

B. Implement security features provided by the suppliers of equipment and systems

We should insist on implementation on the security features in the form of product upgrades. Factory security settings (such as the computer network firewalls) are often adjusted to ensure maximum usability and minimum security. All security functions should be to ensure maximum levels of safety.

C. Conduct internal and external systems of protection against intrusion and establish a 24-hour monitoring system

In order of effectively respond to cyber attacks, it is necessary to establish a strategy to protect against intrusion by notifying the system administrator about a malicious network activity originating from internal or external sources. Monitoring system for detection would be active 24 hours a day, and this feature, which can be easily set up, would send a notice about the attack by sms message or e-mail. In addition, in order to ensure an effective response to any attack, procedure for responding to incidents should be prepared. As a complement to network monitoring, in order to reveal the existence of suspicious activity, it should be possible to record all the daily logs on the systems [8].

D. Establish SCADA "red team" to identify and assess possible scenarios for an attack

Establish a "red team" for identifying potential scenarios of attacks and potential vulnerabilities of the system. Use different profiles of people who can recognize the weaknesses of the whole network, SCADA systems, physical systems and security controls. People who regularly work on the system have a great insight into the vulnerability of SCADA network, and they should be consulted for identification of potential critical scenarios and the possible consequences.

E. Clearly define cyber security roles, responsibilities and authority for managers, system administrators and users

Staff needs to understand specific and define clear and logical roles and responsibilities. In addition, key personnel should be given sufficient authority in the execution of their duties. Establish cyber security organizational structure that defines roles and responsibilities and clearly identify how the cyber security issues escalated, and when notified in an emergency.

F. Document the network architecture to identify systems that contain important functions or contain sensitive information that requires additional levels of protection

As part of the process of establishing an effective protection strategy is necessary to develop and document a robust informational security architecture.

VI. CONCLUSION

The paper explaines the importance of defining the ISC systems as a national critical infrastructure. Also, it shows the frequency, types and vunerabilities of SCADA systems. Parer explains the existing security measures implemented in HPP Perucica, as well as measures that could be implemented for security improvement.

LITERATURA

[1] *Critical Infrastructures and Services*, The Europian Union Agency for Network and Information Security, 2016 https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada?tab=details

[2] Keith S. ,Victoria P., Suzanne L., Marshall A. & Adam H.(May 2015). *Guide to Industrial Control Systems (ICS) Security*, U.S. Department of Commerce : National Institute of Standards and Technology Special Publication, (http://dx.doi.org/10.6028/NIST.SP.800-82r2)

[3] Gleb Gritsai Alexander Timorin Yury Goltsev Roman Ilin Sergey Gordeychik Anton Karpin (2012). *Scada safety in numbers*, Positive technologies

[4] Katherine Brocklehurst (2016). ICS *Vulnerabilities Trend Report: Missed Warnings, exposed industrial environments.* FireEye

[5] *STUXNET Malware Targets SCADA Systems*. Trend Micro. Jan 2012.

[6] *Strategy for Cyber Security in Montenegro*, Government of Montenegro, 2013, pp. 8–9.

[7] *Defense in Depth – Multi-Layer Protection Approach*, Siemens. 2014.

[8] *21 Steps to Improve Cyber Security of SCADA Networks*, U.S. Department of energy, 2012