Specification of the Current State Vulnerabilities Related to Industrial Control Systems

http://dx.doi.org/10.3991/ijoe.v11i5.4981

Jan Vávra, Martin Hromada, Roman Jašek
Tomas Bata University in Zlín, Zlín, The Czech Republic

***Abstract*—The contemporary trend of increasing connectivity, interoperability and efficiency of technologies, which are used in organizations, also affected Industrial Control System (further only ICS). The recently isolated system is becoming more dependent on interconnection with external technologies. This leads to a formation of new vulnerabilities, which are significant threats to ICS. For this reason, it is necessary to devote considerable effort to analyze vulnerabilities. Neglecting of this area could lead to damage or unavailability of ICS services. The purpose of the article is to evaluate vulnerabilities related to individual elements of ICS. The fundamental question of the article is to find a true distribution of security risk related to ICS.**

***Index Terms*—Cyber security, Industrial Control System, Information and Communication Technologies, Vulnerability.**

I. INTRODUCTION

ICS is part of Critical information infrastructure that is why every cyber-attack on these systems can be considered as a lethal attack, which can cause serious damage to the environment, population or financial sector. It can also have a serious impact on the functioning of the state.

The aim of the article is to evaluate cyber threats in relation to ICS. For this reason, there is a research involving analyzed data from a US database of vulnerabilities under the ICS-CERT. Depth vulnerability analysis of any system is an integral part of increasing system resilience. This is particularly important in the case of Advanced Persistent Threat.

ICS elements can be divided into three main layers: business, supervisors, control. The article focuses primarily on an evaluation of vulnerabilities falling within the control and supervisory layer. The purpose of the article is to find out which of the analyzed layer represents greater security risk for ICS.

II. INDUSTRIAL CONTROL SYSTEMS

ICS systems are developed for monitoring, management and control of industrial systems. They are an important part of the critical information infrastructure, which penetrate into areas of transportation systems, power plants, dams, water treatment, oil production, chemicals, gas distribution, etc.

Industrial control systems have a positive influence on contemporary society. ICS is under increasing pressure to improve efficiency and interoperability. It resulted in the emergence of new vulnerabilities. As a consequence, the protected system becomes more vulnerable to new cyber-attacks.

Wide area of ICS can be divided into two main areas. The first of these is geographically independent Supervisory Control and Data Acquisition (further only SCADA) system. The second group is classified as geographically dependent systems such as a Distributed Control System (further only DCS). A summary of the main differences between SCADA system and DCS is shown in the Tab. I.

TABLE I.
COMPARISON BETWEEN SCADA AND DSC [1]

Description of systems	***SCADA***	***DCS***
Orientation	Data-gathering	Process trends
Geographical distribution	Global	Local
Obtaining the necessary data	Always connected to databases	Always connected to I/O devices
Purpose	Coordination of infrastructures	Control endpoint devices
Deployment of the system	Centralized	Decentralized

A. Basic Operations

Detailed specifications of ICS, is a relatively complex operation. For this reason, it is advisable to demonstrate basic operations of ICS in a simplified model. The model is shown in Fig. 1.

All ICS operations are focused on controlling and monitoring processes. The whole model can be divided into three main layers. The lowest layer of the entire system is focused on the physical manifestations of a controlled process. Actuators and sensors are used for monitoring and regulation. This layer is directly connected to a second layer.

The second layer, also called as the control layer is focused on control of processes. It is important to say that programmable logic controllers (further only PLCs) are responsible for controlling processes. They receive real information about the controlled process from the sensors. PLCs based on their programs decide what to do and then give instructions to the actuators, which regulate the controlled processes.

The third layer of the entire ICS is focused on monitoring and collection data relating to controlled processeses. This layer consists of Human-Machine Interface (further only HMI) and Remote Diagnostics and Maintenance. [2] The HMI represents a connection between the system and human operators. Human operators are responsible for

control, regulation and management of the controlled processes. Human operators also receive important information about the current state from PLCs. The purpose of Remote Diagnostics and Maintenance is to identify abnormalities and implement prevention and revitalization measures. [2]

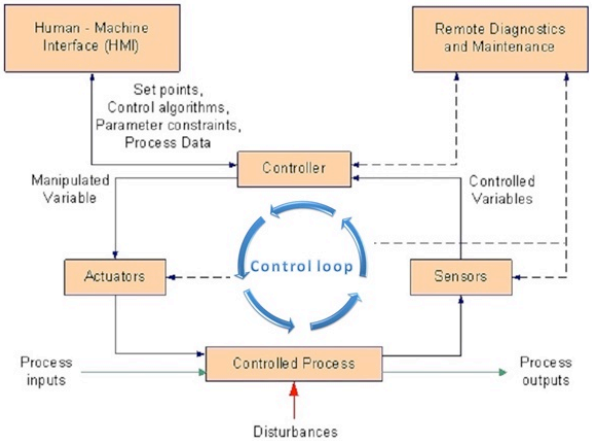

Figure 1. The basic operation of ICS [2]

B. Architecture

It is important to establish three basic layers (business, supervisory, control) for the correct specification of ICS architecture. Layers are further specified by their characteristic features. The individual layers are shown in Fig. 2.

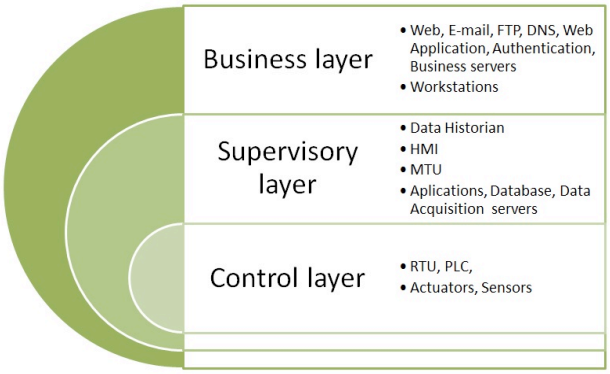

Figure 2. ICS architecture layers [5]

Each of the layers represents a hierarchical management level of ICS. This chapter describes layers including the hardware components themselves.

Security threats arising out of the inadequate implementation of cyber security measures could be misused for cyber-attacks. Various Attack Vectors are used for penetration and distribution of the malicious code in ICS. For this reason, it is advisable and necessary to identify primary paths that are used for penetration into the system. Exploitation of vulnerabilities is the first step to penetrate and compromise the system, which may lead to the collapse and loss of its functionality.

1) Control Layer

This is the lowest layer in the hierarchical management system ICS, which directly monitors and controls industrial processes. There are used multiple sensors and actuators. Furthermore, there is a Remote Terminal Unit (further only RTU) and a Programmable Logic Controller. They are responsible for control and management of industrial processes based on its software.

a) RTU

Remote Telemetry unit is an electronic device used for controlling industrial processes. Its function is similar to a PLC. However, its usage is different. It is a Field Device, which is connected to wireless data transmission. That is why RTU is used where is not possible to use traditional wire solutions.

b) PLC

Programmable Logic Controller is an industrial computer, which is responsible for local control and management of industrial processes. PLCs receive feedback from sensors and then regulate the system through actuators. PLCs have a programmable memory used to store instructions and functions which define their behavior.

c) Actuators and Sensors

These electronic devices are classified as the lowest elements in the hierarchical management system of ICS. Actuators and sensors are devices which have influence and also are influenced by controlled processes. Sensors detect industrial environment and thereafter inform Controller (PLC, RTU). On the other hand Actuators works with inputs which are generated by Controllers.

2) Supervisory Layer

This layer is responsible for monitoring and supervising physical processes. This layer stores and uses important data. Human operators can manage the system via HMI. They use algorithms which modify the behavior of controllers, thereby affecting physical processes.

a) Data Historian

Data Historian is a centralized database of historical data relating to the controlled processes. The data can be used for statistical analysis and evaluation. [2]

b) Human Machine Interface

HMI is the interface between human operators and the controlled system. It is an essential element of management and control within the system. It informs operators about a current status of controlled processes. This comunication requires the necessary data from Data Acquisition Server. HMI is also used to set up parameters which determine controller activities.

c) Application Server

Application Server is responsible for controlling and directing data traffic within applications. Transform data into a correct format which are suitable for communication. It is also responsible for observance of data communication priorities. [2]

d) Database Server

Database Server is a standalone computer where the database lies. The server provided database services to selected applications which are critical to ICS.

e) Data Acquisition Server

Data Acquisition Server provides interconnection between services and Control Layer (mainly PLC and RTU). Received physical data from sensors are sent via a bus to the applications, which are based on the Internet Protocol (IP). This communication is provided by Data Acquisition Server, which allows users to remotely access.

f) Master Terminal Unit

Master Terminal Unit (further only MTU) or the SCADA server is an element, which acts as a master in SCADA systems. On the other hand, elements such as RTU or PLC can be described as a slave. MTU receives data from the RTU / PLC which are further processed as desired. [2]

3) Business Layer

Business Layer is the highest layer in hierarchical management model. This layer using obtained data for a company itself. Especially for increasing profits, streamline marketing, and accounting, administrative and business support. Business Layer is the most dependent layer on connection to the Internet and also can be considered as the most open layer. That is why it is the first target for hackers in order to gain full control over ICS. [3]

There are many topics related to Cyber Security in businesses however, a few are focused on control and supervisory systems. The article deals with the analysis of vulnerabilities falling within Supervisory Layer and Control Layer.

C. Safety Instrumented System

Safety Instrumented System (further only SIS) is developed and used in a close relationship with ICS. Its purpose is to enhance the protection of Critical Process Systems. [1] SIS is an integral part of the critical information infrastructure therefore their failure could have a significant impact on citizens and the state. It is one of the examples where information technology can affect the physical world.

SIS is focused on the prevention of crisis situations however it is not a part of ICS. This system is an ICS supplement. It is responsible for shutting down critical processes. The system is mainly composed of sensors, decision circuits, and control elements. SIS monitoring current state of processes while ensuring it does not exceed predetermined limits. [1]

D. The Main Difference Between ICT and ICS Cyber Security

There is one question that must be answered. What are the main differences between ICT and ICS cyber security? This problem is described by using basic security criteria: availability, confidentiality and integrity. Their relationship to ICS and ICT are shown in Fig. 3. It follows that confidentiality is the most important for ICT. On the other hand, availability is the most important for ICS. That is why the most important threats for ICS are not so significant for ICT.

Figure 3. Comparison of ICT and ICS cyber security [1]

III. METHODS

The purpose of the research is to evaluate the ICS vulnerabilities. The data was recovered from vulnerability database ICS-CERT for the period from 01. 2015 to 02. 06. 2015.

The data are an essential basis which is decisive for the statistical assessment of Supervisory and Control layer. There are analyzed approximately fifty vulnerabilities.

The main question of the article is: "Which of the investigated hierarchical layers represents a greater threat in terms of cyber security. The question is examined according to following criteria: number of reported vulnerabilities, type of cyber-attacks, depending on vulnerabilities and their severity. In conclusion, there are two analyzes, which are focused on Exploitability Metrics and Impact Metrics.

IV. RESULTS

In order to evaluate the main objective of the research, it was necessary to specify the individual layers. Each of layers is divided into individual elements (shown in Fig. 2). Research data are classified into predefined groups (shown in Fig. 4). The graph shows the distribution of vulnerabilities per layer and vulnerability related to individual elements.

We can say that the most vulnerable layer is Supervisory with 64% of the total vulnerabilities, and the most vulnerable element is HMI with 36% of vulnerabilities. On the other hand, cannot omit Control Layer with 36% of vulnerabilities, and the most vulnerable element PLC with 18% of vulnerabilities.

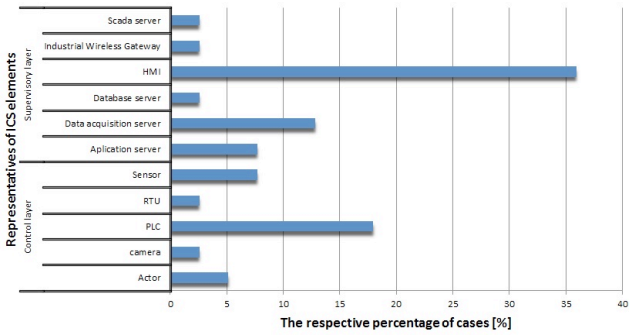

Figure 4. The distribution of vulnerabilities [5]

The second objective of the research is to describe the possible consequences of identified vulnerabilities. The distribution of impacts is shown in Fig. 5, where are the individual impacts divided into separate layers.

The result of this investigation demonstrates that the most common impacts on the supervisory layer are Obtain Information with 13% of vulnerabilities and Gain Privileges with 13% of vulnerabilities. It can, therefore, be established that this layer is very vulnerable to privilege escalation, which allows an attacker to break into a secure system. The Control Layer is the most affected by Denial of Service (further only DoS) with 17% of vulnerabilities and Gain Privileges 11%.

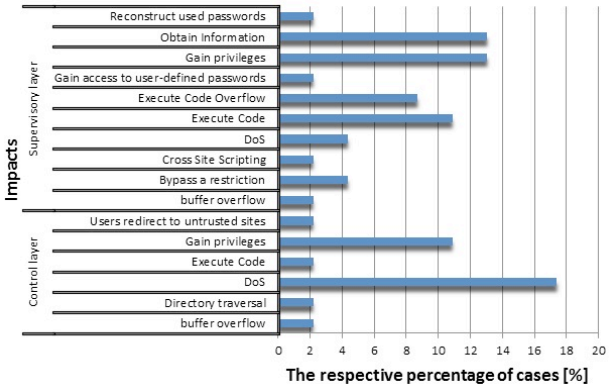

Figure 5. The distribution of impacts [5]

The third objective of the research is concerned with the severity of vulnerabilities. To this end, we use standard vulnerability assessment: Common Vulnerability Scoring System (further only CVSS) version 2. Vulnerabilities are evaluated by six CVSS metrics, which are used for the research (shown in Fig. 7 and Fig. 8). Every single vulnerability is categorized on scale of 0 to 10. The least significant vulnerability is represented by 0. However, the most significant vulnerability is represented by 10. There are five intervals for every layer. These intervals are established for vulnerabilities according to CVSS. [4]

As it has already explained, the largest number of vulnerabilities falls within Supervisors Layer. However, in Fig. 6 we can see that Supervisory Layer also excels in severity and hazard, which are arising from vulnerabilities.

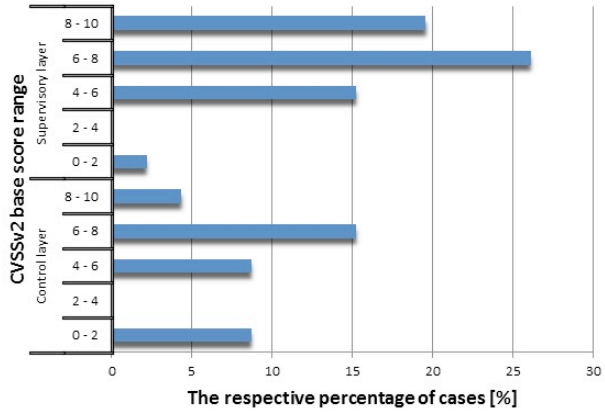

Figure 6. The distribution of vulnerabilities severity [5]

There are two figures (Fig. 7 and Fig. 8) which representing six metrics used to calculate CVSSv2. These are the following areas: Access Complexity, Access Vector, Authentication, Confidentiality, Integrity and Availability. These metrics are divided into two main groups: Exploitability Metrics and Impact Metrics.[4] Exploitability Metrics are used in Fig. 7 for analyzing vulnerabilities. Exploitability Metrics are divided into three subgroups: Access Complexity, Access Vector and Authentication. [4] They are used for defining and evaluating vulnerability according to strictly defined criteria.

Access Complexity metric describes the degree of the special conditions that must occur in order to exploit the vulnerability. [4] For this reason, Access Complexity is divided into three areas according to the level of initial conditions. The analyzed data show that a considerable part of vulnerabilities (55% of Access Complexity cases) do not need to abuse other special conditions (shown in Fig. 7).

The purpose of Access Vector is to evaluate what approach attacker must achieve to exploit vulnerabilities. The metric is divided into three areas. Attacker must have local access to exploit vulnerability (Local). An attacker must have access to networks in which there is a system with vulnerability (Adjacent Network) or may not have physical access to the LAN (Network), which leads to remote abuse. [4] The results of investigation show that the largest number of analyzed vulnerabilities can be remotely exploited (59% of Access Vector cases).

Authentication is the third metric which is used for the research. Vulnerabilities are divided according to whether they need perform authentication once, several times or not needed to carry out which is the basic assumption for their misuse. [4] The largest group of analyzed vulnerabilities can be exploited without authentication to 84%.

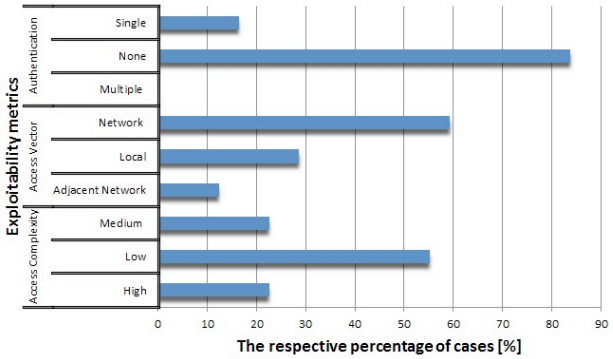

Figure 7. The distribution of Exploitability Metrics [5]

The final part of the article is focused on the specification of ICS impacts based on the analyzed data. This issue describes the group of metrics known as Impact Metrics. The impacts are divided into three subgroups that represent different metrics: Integrity, Confidentiality, Availability.[4] Each vulnerability is defined within individual metric. Each metric is represented by one of these values: none, partial or full impact on the integrity, confidentiality or availability.

The evaluated data shows that vulnerabilities have the largest impact on Availability. It may cause complete loss (51% of all vulnerabilities) of system availability. This movement should be also seen in other Impact Metrics, which are confidentiality (43% of all vulnerabilities) and integrity (45% of all vulnerabilities).

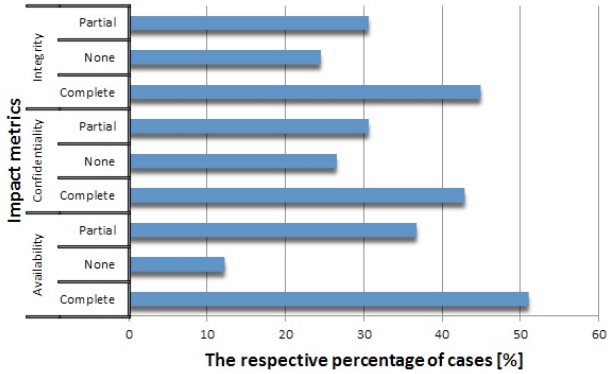

Figure 8. The distribution of Impact Metrics [5]

V. CONSLUSION

The purpose of the article is to evaluate the vulnerability in relation to ICS. It is therefore necessary to set the objectives that are subsequently examined. The assessment of the vulnerabilities is performed according to different perspectives.

Research indicates that Supervisory Layer is more vulnerable than Control Layer. It can be demonstrated on number and severity of vulnerabilities. These can be exploited which leads to penetration into the system. However, it is important to warn about a high number of vulnerability, which may lead to DoS which cause a serious threat to the availability of services. It is the most important safety criterion for ICS. This opinion is enhanced by the fact arising from the Impact Metrics analysis. It is noticeable that the analyzed vulnerabilities have the greatest impact on availability. This is even more enhanced by the fact that most of the analyzed vulnerabilities can be remotely exploited and do not need any authentication.

ICS cyber-attacks will become a more serious threat to the population and the countries themselves. For this reason, it is logical and effective to prevent them. It can partly be achieved by thorough analysis of vulnerabilities.

ACKNOWLEDGMENT

First and foremost, I would like to thank Ing. Martin Hromada Ph.D and Assoc. prof. Mgr. Roman Jašek, Ph.D. for their support and mentoring. They kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper.

REFERENCES

[1] MACAULAY, Tyson a Bryan SINGER. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS.* Boca Raton, FL: CRC Press, c2012, x, 193 p. ISBN 14-398-0196-7.

[2] STOUFFER, Keith, Joe FALCO and Karen SCARFONE. *Guide to Industrial Control Systems (ICS) Security* [online]. [cit. 2015-01-31]. Available: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, National Institute of Standards and Technology, 2011.

[3] KNAPP, Eric. Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA , and other industrial control systems. Waltham, MA: Syngress, c2011, xvii, 341 p. ISBN 15-974-9645-6.

[4] MELL, Peter, Karen SCARFONE and Sasha ROMANOSKY. *A Complete Guide to the Common Vulnerability Scoring System Version 2.0* [online]. 2007 [cit. 2015-07-18]. Available: https://www.first.org/cvss/cvss-v2-guide.pdf

[5] *Ics-cert: Industrial Control Systems Cyber Emergency Response Team* [online]. [cit. 2015-07-20]. Available: https://ics-cert.us-cert.gov/

AUTHORS

Jan Vávra, Martin Hromada, and **Roman Jašek** are with Tomas Bata University in Zlín, Zlín, The Czech Republic.

This work was founded by the Internal Grant Agency (IGA/FAI/2015/042). Submitted 21 August 2015. Published as resubmitted by the authors 20 September 2015.