"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 2
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

SECURITY OF INDUSTRIAL CONTROL SYSTEMS – AN EMERGING ISSUE IN ROMANIA NATIONAL DEFENSE

Emil PRICOP[1]
[1]Automatic Control, Computer & Electronic Engineering Department Petroleum-Gas University of Ploiesti

Abstract: *Romania, a NATO country since 2004, is situated at the Eastern NATO borders, having a geostrategic position at Black Sea and near Ukraine, a very sensitive area due to its vicinity and influence of Russia. Romanian energy production and distribution systems along with industrial plants are critical infrastructures for the country energetic independence, an important factor of national defense. Each power plant, petrochemical facility or refinery is operated by various interconnected control systems. In this paper the author tries to address the critical industrial control system protection against cyber-threats (cyberterrorism, cyberwar, hackers, etc.). The state of the art in identifying vulnerabilities and securing control systems is presented in the first part of the paper. Based on the analysis of the identified vulnerabilities the author tries to provide a comprehensive guideline for increasing the security of those critical infrastructures without affecting their performances and functionality.*
Keywords: *control systems security, cyber-threats, cybersecurity*

INTRODUCTION

Romania is a NATO (North Atlantic Treaty Organization) member since 2004. It is situated at the Eastern NATO borders, having a geostrategic position at Black Sea and near Ukraine, a very sensitive area due to its vicinity and influence of Russia. Romania is well known for its petrochemical industry: facilities for oil extraction and transport, refineries, chemical and petrochemical plants that can assure its energetic independence. All these industrial facilities integrate various automatic control systems. The biggest refineries in Romania are located in the close nearby of Ploiesti, one of the largest cities of Romania and at 60 km from Bucharest the capital city. Also a nuclear plant was built in Cernavoda, in the vicinity of Bulgarian border and the Black Sea (approximately 70 km). All those industrial facilities are critical infrastructures for Romania economy.

Theindustrial control systems are nowadays very complex systemscomposed by not just sensors, transducers and classical controllers, but also industrial computers, PLCs with networking capabilities, HMIs and various other intelligent devices. All the components are interconnected via Ethernet or wireless networks and are frequently linked to the Internet by various proprietary and public protocols.

SCADA systems are a special class of control systems which are connected to the Internet and can be operated by remote commands from anywhere in the world. All the petrochemical plants, the nuclear and electrical power plants use SCADA implementation for their operation, these systems being vulnerable to various types of cyber attacks.

Since the last years all the control systems were designed and built having as the primary objective the performances. The increasing number of vulnerabilities along with the cyber-threats (cyberterrorism, cyberwar, hackers), the availability of systems documentation and sometimes even the source-code for control systems software components are the reasons why the control systems should be now designed taking into account their security. This is a recent challenge for both industry and academia.

In this paper the author tries to address the critical industrial control system protection against cyber-threats (cyberterrorism, cyberwar, hackers, etc.). The first section of the paper shows which are the critical industrial infrastructures that need special attention. The second section presents an overview of the control systems vulnerabilities. In the last part of the paper the author tries to give a short guideline for securing critical control systems.

CRITICAL INDUSTRIAL INFRASTRUCTURES

The term infrastructure defines the backbone of any entity, the support needed for working and relationating with other entities. Infrastructures can be divided by their role and importance for the stability and functionality of systems into three broad categories:

- common infrastructures, meaning the elements each country can have such as roads, bridges, cities, schools, libraries, etc. During their evolution and depending on the economic and geostrategic context elements from this category may become special or critical entities;
- special infrastructures comprise the entities that are crucial to systems and processes functioning;
- critical infrastructures are the entities thathave a vital role in assuring the safe and secure functioning of economic, social, informational and military processes [1].

In this paper we address the critical industrial systems. US Department of Homeland Security defines the critical infrastructures as all the systems and networks that are so vital that their

incapacitation would have a debilitating effect on security, national economic security, public health or safety [12].

The critical infrastructures include, but are not limited to [1], [12]:

- energy production facilities;
- power grids (electric energy distribution networks);
- water production and distribution and wastewater transportation systems;
- healthcare facilities;
- nuclear reactors and nuclear waste management;
- chemical sector facilities, including petrochemical plants, pharmaceutical manufacturing, chemical substances storage;
- emergency services, such as ambulance, firefighters and police;
- communications systems;
- defense systems manufacturing;
- agriculture, food production and distribution chain;
- financial services.

Each of the critical systems mentioned above integrate one or more control systems. In the following section the author will provide a short overview on the control systems security.

CONTROL SYSTEMS OVERVIEW

A system is an assembly of entities that interact each other and with the externalenvironmentin order to achieve a specified goal. A control system is a technical system that is able to monitor and regulate a process or an industrial installation without the direct human intervention.

The system functioning is based on information transfer between the exterior, the systems and its components. In control system by information is understood any qualitative or quantitative parameter that can be used to characterize the system behavior. For an automated system the information transfers are realized by using different kind of signals, mainly electrical.

In figure 1 is presented a simple control system block diagram that reveals the signals transferred between the systems components and with the exterior systems. The fundamental system elements are presented in the block diagram. The controller receives the prescription as an input and using a control algorithm elaborates the command signal, based on the feedback measured from the process. All those signals are informational signals that are exchanged between system elements. It is obvious that all this information can be manipulated in a cyber attack, leading the control system to not be able to achieve its objective. Moreover a wrong calculated command system can lead to an industrial accident with possible severe impact on human lives, industrial facility and environment.

The development of electronics, computer science and telecommunications allowed the control system evolution. Nowadays the control systems are not simple and independent entities, but they are hierarchical and distributed systems with a strong communication infrastructure. Moreover they are connected with production planning systems such as ERP and CRM and are frequently operated by remote specialists, by using VPN or Internet connection. In this context the control systems are becoming real targets of the cyber-attackers.

In this context a hierarchical model of control systems in a big factory is provided. This approach is derived from International Society of Automation – ISA-95 standard.[4]

The model has 5 layers containing both automatic control and economic key factors. The top-most level is represented by the *economic superior-layer*, which is strictly related to the national economy. Information about the market needs is exchanged at this level, receiving production request and sending acquisition orders.

The *ERP systems* layer is subordinated to the economic superior layer. At this level the production is scheduled, the necessary resources are reserved in order to satisfy the request from the economy. Also this level should be able to provide information about the raw materials that are needed in order to accomplish the objectives.

The centralized controllayer is the first level where true technical control systems are located. This

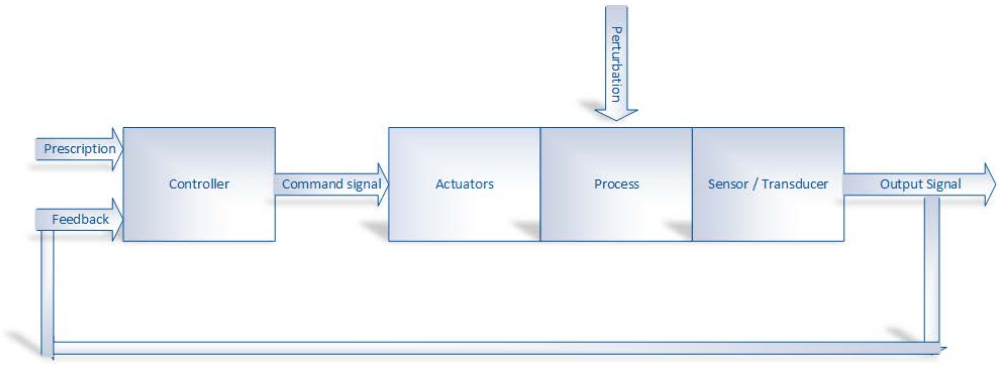

Figure 1 – Control system block diagram

layer is a barrier between the economic and industrial systems, since at this level economic objectives are converted into technical objectives. This layer is also the centralized control point for the whole installation. It collects data from the inferior level (distributed control systems) and coordinates the functions of all the systems in the factory or plant. At this layer are placed various implementations of SCADA systems, journaling and reporting modules, historian, etc.

At this point are implemented also remote control systems that represent a real vulnerability for the whole control infrastructure.

The *automation equipment* layer represents the next level. Here are located all the equipment directly responsible with process control, such as PLCs, process computers, controllers and specialized processing units. Equipment situated at this level should communicate with the superior centralized control devices and also with the sensors, transducers and actuators at the inferior layer. Specially designed protocols along with Ethernet IP are used to implement the communication facilities.

The down-most layer of the proposed system is represented by *field equipment*, such as sensors and actuators, devices that are linked directly with the process. On this level is implemented a true network for measurement, data acquisition and command distribution between controllers, sensor and actuators. The protocols used on this layer are particular such as BITBUS, Profibus, DeviceNET, CANOpen, InterBUS, Modbus or Field Bus.

A suggestive representation of this hierarchical model is presented in figure 2.

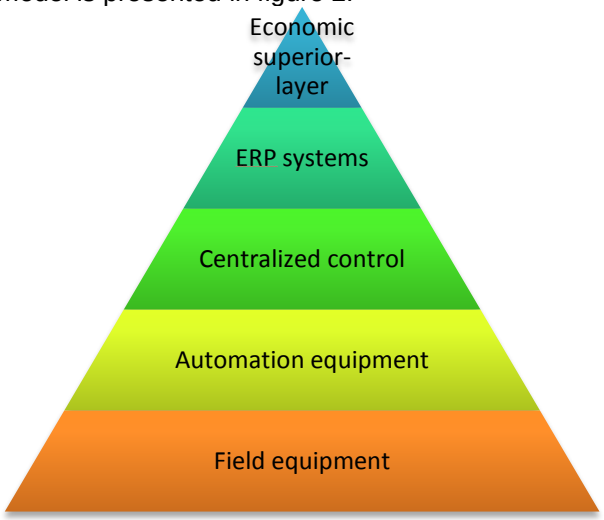

Figure 2 – Hierarchical model of a complex control system

Each layer communicates with its superior and inferior layer, exchanging critical information for good system functioning. The entities situated on each level communicate using network protocols in order to synchronize and exchange data. We can say that the main task associated with assuring control system security is to assure the security of the networks utilized by the automation infrastructure.

CONTROL SYSTEMS SECURITY CONCEPTS

There should be made a clear distinction between the two fundamental concepts of *safety* and *security*[2]. Safety refers to the ability of the system to harm people when an error or a random error occurs. The security, which is the object of this paper, consist of the ability of the system to not cause any kind of loss in case of the occurrence of deliberate malicious acts against the system. Those two attributes form an assembly that is critical for the correct system functioning [3].

A system with high reliability and maintainability, but that lacks security, being vulnerable to cyber attacks, will surely generate economic losses for its owner. On the other side a very secure system, but lacking the ability to recover rapidly after an incident or with little reliability is not efficient. Taking into account these statements we can conclude that there should be found equilibria between the two attributes: safety and security.

In other words we can say that the main challenge for researcher and industry is to assure a good security level to control systems without affecting their efficiency and their ability to reach their main objective (monitoring, control, etc.).

The control systems security can be defined as the lack of vulnerability to vandalism, tempering, sabotage, informatics viruses and worms, cyber attacks and other electronic threats.[4.]

It is obvious that this objective can be reach by using two means:

- physical access control mechanisms and usage rights allocation systems;
- information security, meaning all the countermeasures taken to protect form cyber threats and to assure data authenticity, confidentiality, integrity and non-repudiation.

A threat – vulnerability analysis should be done, in order to correctly identify the security needs and the required measures that are to be implemented.

Threats are mainly the attackers, represented by people, malicious computer / PLC software, or other systems.Threats are characterized by a high degree of indetermination and their quantification is a very complex and difficult task. The threats apparition cannot be prevented or controlled.

Vulnerabilities are security breaches in the control system that can be exploited by a threat in order to gain access or to make the system unavailable. Opposite to threats, the vulnerabilities can be controlled, detected, estimated and quantified by risk analysis, as presented in [6]. The system owner can protect the system against known vulnerabilities.

CONTROL SYSTEMS VULNERABILITIES AND COUNTER MEASURES

Using two-factor authentication of persons can solve the physical access control issue. This method is well described in [7] and [8] and consists in using a biometric characteristic (fingerprint or iris template) along with a PIN or a password for precise employee identification. This approach is not in the scope of the presented paper.

Assuring the information security in control systems remains the main challenge for researchers, academia and even industry. The big number of cyber attacks that took place in the last two years make us trust that cybersecurity of industrial systems is a new research domain in a continuous and rapid evolution.

The literature and security companies reports a large number of security incidents starting from the script kiddies who tries to gain access to some public system to real cyber terrorism or cyber war episodes, such as the spreading of Stuxnet, Duqu or Flame worms.[4]

In the following paragraphs the main vulnerabilities and types of attacks against control systems along with the corresponding countermeasures will be presented.

FIELD LEVEL COMMUNICATION PROTOCOLS VULENRABILITIES

Communication at the field level is done using specialized protocols such as Modbus and Profibus. Each of these two protocols was analyzed and specific vulnerabilities were identified.

Modbus is an application level protocol that allows data transmission in industrial networks by using a client/server approach. Modicon Company, a PLC devices producer, defined the protocol in 1979. The protocol has three versions Modbus ASCII and RTU, where data is transmitted using RS485 in ASCII respectively binary format, and Modbus/TCP, that encapsulates standard Modbus messages in TCP/IP packets4], [5], [10]. In figure 3 is presented a block diagram of a control system with integrated Modbus communication in RTU and TCP versions.

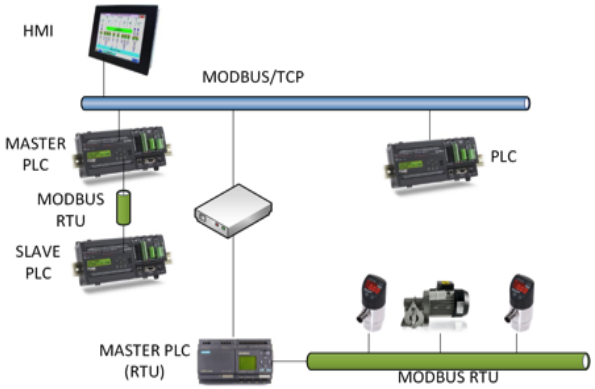

Figure 3 – Block diagram of a control system with Modbus RTU communication between sensors/actuators with PLC and Modbus TCP between PLCs

The most critical protocol vulnerabilities are:

- Lack of a message source authentication mechanism, allowing an attacker to hi-jack a sensor and to inject malicious data;
- Lack of a message destination confirmation mechanism (impossibility to assure the confidentiality of data);
- Lack of an standardized encryption mechanism for transmitted messages;
- The possibility to re-program PLCs via Modbus connections, since there is no authentication mechanism implemented [4].

In order to respond to the vulnerabilities it is obvious that a sensor authentication mechanism should be implemented. This is a complex task since any modification at the protocol level will lead to changes in the automation equipment that have Modbus communication capabilities.

It is possible to implement such a system by using hash functions and HMAC on Modbus devices and sending the generated string together with the data.

Another approach is to implement an automated traffic analysis system on Modbus communication lines. The system should detect and block each Modbus message that has incorrect length, reset codes, function codes to interrogate and list the equipment connected to the line, function codes that list the current configuration of the equipment or function codes for listing all the commands that are recognized by a specific device.

Profibus (PROcess FIeld BUS) is a very well established communication protocol for interconnection of sensors, transducers, actuators, intelligent equipment, controllers, PLCs and HMIs. The standard is open and its development started in 1989. Currently there are used many versions of Profibus, the most significat being Profibus DP, Profibus FMS and Profibus PA [11].

Profibus protocol is implemented at level 2 (data link layer) and 7 (application) of the ISO-OSI model for communication networks.
Profibus vulnerabilities are mainly caused by the lack of a authentication mechanism for each connected device. An attacker can create a false master node that can take over the whole network.
A very good example of Profinet vulnerabilities exploitation is the Stuxnet work, which affected master nodes (PLCs). The worm is very well described in [4].
The common way to protect the Profibus network against cyber threats is to isolate it from the production network of the factory. Also it is important to isolate each Profibus network segments, in order to assure that compromising a master node on a segment will not affect the rest of the nodes.
Another important challenge is to implement a powerful authentication and encryption mechanism over standard Profibus.

TCP/IP THREATS, ATTACKS AND COUNTERMEASURES

TCP/IP is also used frequently in the process control network not only at the higher layer (economic layer, centralized control) but also at the automation equipment level.
The most common attack types in TCP/IP networks are:

- Sniffing attacks – intercepting and decoding network traffic to discover sensitive information;
- Denial of Service (DoS) –interrupting the functioning of a system or making a informational resource unavailable;
- IP spoofing – forging an IP address used as the source of data packets in order to impersonate a valid sender [5], [9]

Sniffing attacks are very common and easily to conduct since now there are a variety of tools available on the market for this purpose, for example the open-source software Wireshark. This kind of software is frequently used by network administrators for monitoring the network traffic for abnormal activity, but it can be also used by a malicious user in order to obtain sensitive information that transit the network. The attack is a passive one, since data is only read, not modified in any way.
The attacker has to obtain physical access to the network to install the software. The software will then commute the network interface card (NIC) in the so-called promiscuous mode, in which all the packets in the network are intercepted by the NIC. Then the attacker has to detect automatically or manually sensitive data transmitted as clear text such as passwords, encryption keys, usernames or various configuration parameters for connected automation equipment. The data may be used to obtain access or take over the system.
The best way to protect the network for this kind of attack is to always use data encryption. It is recommended to use SSL / HTTPS instead of simple HTTP sessions. The transmission of encryption keys should be done over secured and authenticated channels, by using specific algorithms such as Diffie-Hellman.
The network administrator should always check the entities that are connected to the network in order to discover any suspect activity.
Denial of Service are active attacks that are used in order to make a resource unavailable. The most frequent attack mechanism is to send a large number of requests to a system (flooding).
This type of attack can be prevented by a well-configured and powerful (usually hardware) firewall. The firewall should block any suspect activity such as a large number of connections opened by a client or a large number of half-open TCP connections.
Installing redundant resources (servers, master nodes) and dynamic resource allocation is another approach to mitigate the effects of a DoS attack.
IP spoofing attacks consists of forging the TCP/IP packets in order to be identified as valid and sent by an authorized user. The attacked system will consider the packet to be valid and will answer the attacker request. This attack method can be used to take over a system or a wireless sensor for example. The best method to protect from this type of attack is to filter the nodes in the network by their MAC address and always to check the correspondence of MAC and IP in any received data packet.

CONCLUSIONS

Critical infrastructures are the backbone of the entire economy of a country. Nowadays the critical infrastructures integrate various automated control systems containing process computers, PLCs, intelligent sensor and networked elements. These systems are very complex and are often the target of malicious attackers from script kiddies and disgruntled employees to cyber terrorists and, sometimes, enemy armies.
The security of the control systems in critical infrastructure is becoming a national defense issue. The power grid, the chemical facilities and water distribution system are only three examples of infrastructures that are crucial not only for the well functioning of the economy but also for human lives. These infrastructures are often victims of cyber attacks.

In this paper the author tries to present the basics of control systems security. The information security threats and vulnerabilities at the field equipment level (Modbus and Profibus protocols) are analyzed in this work. For each of the two protocols security measures are mentioned. The last part of the paper focus on TCP/IP network security, given that much automation equipment in use nowadays is integrated in TCP/IP networks.

Further research should be done for securing the low-level protocols such as Modbus, Profibus, Profinet, DeviceNet, CANOpen, especially in regard to the autehentication of the interconnected devices.

BIBLIOGRAPHY:

[1] Alexandrescu G., Văduva, Gh., Infrastructuricritice. Pericole, amenințări la adresaacestora. Sisteme de protecție.,EdituraUniversitățiiNaționale de Apărare "Carol I", București, 2006

[2] Hessami, A.G., A Systems Frameworkfor Safety & Security, The Holistic Paradigm, Systems Engineering-The Journal of the International Council on Systems Engineering, Volume 7 Number 2, 2004, pp 99-112

[3] Hessami, A.G., Cybernetic safety & security, a new paradigm, Cybernetic Intelligent Systems, 2008. CIS 2008. 7th IEEE International Conference on, vol., no., pp.1,10, 9-10 Sept. 2008

[4] Knapp, E. Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems, Syngress, USA, 2011

[5] Mackay S., Wrigth E., Reynders D., Park J. - Practical Industrial Data Networks - Design, Installation and Troubleshooting, Ed. Newnes, 2004

[6] Pricop, E., Mihalache, SF, Assessing the security risks of a wireless sensor network from a gas compressor station, Electronics, Computers and Artificial Intelligence (ECAI), 2014 6th International Conference on, 23-25 Oct. 2014, pp. 45-50

[7] Pricop, E., Biometric identification of persons – A solution for time & attendance problems, Sesiunea de comunicăriştiințifice IMT 2008, Universitatea din Oradea, Băile Felix, mai 2008

[8] Reid, P, Biometrics for Network Security, Prentice Hall PTR, 2003

[9] Tanenbaum A., Computer Networks (4th ed.), Prentice Hall Professional Technical Reference, 2002

[10] Modbus Specifications, Modbus Inc. www.modbus.org

[11] Profibus Specifications, Profibus&Profinet International, www.profibus.com

[12] US Homeland Security Department Website – Critical Infrastructures - http://www.dhs.gov/critical-infrastructure