CPQ Medicine (2020) 10:5
Review Article

# Industrial Control Systems: The Biggest Cyber Threat

Christos Beretas, P.

*PhD Candidate (Full Scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France*

***Correspondence to:** Dr. Christos Beretas, P., PhD Candidate (Full Scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France.

## Copyright



Received: 19 October 2020

Published: 28 October 2020

**Keywords:** *Industry; Control Systems; Security; Privacy; Attack; Vulnerabilities; Energy*

## Abstract

Industrial control systems (ICS) are critical, as in these systems, cyber threats have the potential to affect, disorganize, change their mode of operation, act as an information extraction vehicle, and ultimately turn against itself. creating risks to the system itself, infrastructure, downtime, leakage of sensitive data, and even loss of human life. Industrial control systems (ICS) are vital to the operation of all the modern automated infrastructure in the western world, such as power plant and power stations. Industrial control systems (ICS) differ from the traditional information systems and infrastructures of organizations and companies, a standard cybersecurity strategy cannot be implemented but part of it adapting to the real facts and needs of each country, legislation and infrastructure. These systems require continuous operation, reliability and rapid recovery when attacked electronically with automated control, isolation and attack management processes. Incorrect settings and lack of strategic planning can lead to unprotected operation of critical installations, as they do not meet the cyber security requirements. Industrial control systems (ICS) require special protection in their networks, as they should be considered vulnerable in all their areas, they need protection from cyber attacks against ICS, SCADA servers, workstations, PLC automations, etc. Security policies to be implemented should provide protection against cyber threats, and systems recovery without affecting the operation and reliability of operating processes. Security policies such as security assessment, smart reporting, vulnerability and threat simulation, integrity control

analysis, apply security policy to shared systems, intrusion detection and prevention, and finally firewall with integrated antivirus and sandbox services should be considered essential entities.

## Introduction

Industrial Control Systems (ICS) must be installed in isolated environments away from both physical and cyber threats. Unfortunately, this is not always happened. This can be demonstrated by using specialized cyber security tools to look for central ICS Servers whose management platforms are exposed to the Internet without security policies leaving exposed installations behind a username and password which is easy to violate and manage this system to fall into the hands of strangers with incalculable consequences. Industrial Control Systems (ICS) are found in areas such as: energy, aerospace, oil, chemicals, automotive, etc. More than 90.0% of these ICS servers have vulnerabilities, which can be exploited even remotely or local as they offer sometimes complete remote management and on the other hand the facilities themselves manage each other management data or operation with insufficient or no security at all. Attacks on Industrial Control Systems (ICS) are not the exclusive prerogative of less developed countries, one might wonder a less developed country does not have the funding and knowledge required to secure such systems. In addition to the notorious 2015 attack on the electricity company in Ukraine, which proved to be frightening in scale and size, due to the lack of a strategic cyber security plan and basic security knowledge and dealing with emergency and serious cyber attacks, this was followed by the attack on the steel plant in Germany and the Frederic Chopin airport in Warsaw. The above points out that the attacks themselves have existed, exist, and will intensify in the future because such a large-scale attack in an unsafe system can easily have a huge impact and affect the stability of services and governments [1,2].

The more a country relies on Industrial Control Systems (ICS), the more likely it is to have security vulnerabilities. By their very nature, Industrial Control Systems (ICS) contain different but interconnected components, which are connected to the Internet and contain security vulnerabilities. There is no 100% certainty that an Industrial Control System (ICS) unit will not have security vulnerabilities at some point. However, this does not mean that there is no way to protect against a cyber attack for example a power plant [3,4].

## Problem Definition

Some of the countries where Industrial Control Systems (ICS) are located have the law of missing laws governing security and how to deal with a cyber attack. These crucial facilities employ people who do not have enough knowledge to manage critical situations, which is due to the lack of knowledge transfer or lack of training so that they can perform to the maximum. In addition to cyber attacks on either IoT devices or software security vulnerabilities, the human factor remains an important factor in the security of Industrial Control Systems (ICS). The human factor is capable of jeopardizing an Industrial Control System (ICS) because employee errors or unintentional misconduct were behind incidents affecting the operating networks of industrial control systems (ICS). Over time the systems become more complex but also more functional with automated functions this implies increased protection against cyber attacks and further knowledge of management staff. Both the specialized staff and the system upgrades are two alien entities which can

neither be restricted nor ignored because if one of the two entities is ignored there will be a significant problem of security and smooth operation. The implementation of the Industry 4.0 standard will significantly improve the security of industrial control systems (ICS) as the standard defines the management of smart tools by exchanging information autonomously and controlling each other machine, thus limiting the human factor without eliminating completely, for this reason, in order to have the necessary level of protection, the training of the staff is necessary in order for there to be a smooth operation, something that unfortunately is not often implemented following the logic "since it works, do not touch it" [5].

Industrial Control Systems (ICS) staff often perform dual tasks, which means that a computer security officer is considered to be knowledgeable about security and thus oversees the security of industrial control systems (ICS). something that is wrong. This kind of approach can bring huge digital risks as there is a significant difference in how to deal with digital attacks, network security, as it is difficult for a computer security officer to oversee the security of such critical industrial infrastructure as it lacks architectural knowledge. machine to machine data, lack knowledge about proper cyber configuration and secure integration of machines in the rest of the network, identifying and correcting security vulnerabilities and finally its lack of response to a serious cyber attack. Critical infrastructure managers need to understand the dangers of a critical infrastructure as well as the more critical the infrastructure, the more attractive it is to would-be intruders. Therefore, they need specialized knowledge, adopting a holistic, multi-layered approach that combines cyber protection and specialized training of security specialists, as industrial power plants, for example, will remain safe and fully operational even after a cyber attack. Finally, the application of Industry 4.0 requires the use of IoT, which further complicates security, as it was mentioned in my previous research article on IoT security, they are extremely insecure and need special study on their use in terms of security. their functions as well as their safe integration into the industrial systems. Targeted attack on Industrial Control Systems (ICS) is irrelevant, no potential intruder is satisfied with the infection of a computer, or a server in an industrial infrastructure, the reason is that such an attack does not deal a significant blow to the target industrial infrastructure, the second reason is that the intruder does not have the reception or it is monetary in the form of liters from the target industrial infrastructure nor the reputation he/she would like. The target of the attacker remains the installation of malware which will be installed on distributed systems whether it will be installed by system breach remotely or in the form of phishing. Lack of employee training, lack of security updates, detection of strange connections and processes combined with lack of security policy, attacks on Industrial Control Systems (ICS) find their target [6].

## The Importance of Industry 4.0

Based on what mentioned in the above paragraphs, conclude that the human factor remains a significant threat, but is not solely responsible for the attacks on Industrial Control Systems (ICS) as there are other parameters to lead such a system exploited by the intruder such as incorrect system configuration. Industry 4.0 is designed to fill this gap as introduce Internet of Things (IoT) into Industrial Control Systems (ICS) oversight. IoT security is lacking and needed for installation as well as for specialized configuration and installation in points behind network security systems. Industry 4.0 includes the philosophy of reducing the human factor in combination with enhanced machine safety, this is achieved by the autonomous communication of machines exchanging operating elements with each other, after an authentication method

has been performed so that one machine can certify the validation of the other machine so that they can interact. It is a **Cyber Physical System** that allows to perform functions and decide on the required functions on its own by offering the most transparent operating characteristics. The implementation of Industry 4.0 can provide a detailed and complete picture of the infrastructure, such as smart devices that work, their performance can be checked, operation statistics can be extracted, checking of correct operation, checking of machines, checking the correct use of machines, information analysis, performing diagnostics on the infrastructure, and finally a complete picture of the management and detection of strange connections and processes. The disadvantage in applying Industry 4.0 is the different philosophy followed from country to country, there are countries with different perceptions about the use of Industrial Control Systems (ICS), there are countries that have lacked legal status, other countries are limited in use of automated digital technology, finally other countries show legal attachment to the location of data storage and processing whether they are within their infrastructure or in the Cloud [7].

## Solution

Before the advent of inustry 4.0 but also after, some strict security policies are required which are presented below and aim to ensure both the operation of the infrastructure and the security of data and systems. According to the analysis presented above, the following actions are considered necessary.

• Creating a cyber security policy from the country where the industrial production systems are based, the security policy should include the rules, actions and activities to be done before, during and after a cyber attack. Cybersecurity policy should be reviewed periodically.

• A clear legal framework that defines it is security, personal data, and what is considered confidential.

• Defining employee access levels, which employee has access to which, for how long and the type of access.

• Define access to systems depending on the level of employees.

• Regular checks on systems which are scheduled and also extraordinary.

• Securing sensitive systems and smart devices behind security equipment such as Firewalls.

• Internal security policy which is in line with the country's security policy.

• Identify vulnerable systems and repair them immediately, or put them out of operation as they are a vulnerable point of entry.

• Exclude remote system management, systems will only be remotely managed from specific IP addresses and by entering credentials other than passwords such as public / private key and only from specific individuals.

• Restrict access to internal systems and networking devices such as routers, USB ports, IoT, and peripherals.

• Encrypt sensitive information, decrypting it will be done automatically when searching for data, whether it is a database or files.

• Protection systems such as antivirus, firewall, sandbox, intrusion detection and prevention remain active and up to date.

• Prohibition of installing unauthorized applications.

- Restrict internet access.
- Establish a monitoring team to review compliance with security policies.
- Daily tasks monitoring.
- Physical preservation of facilities.
- Search for security methods used in the past that have succeeded.
- Finally, provide high quality training to all staff to keep them informed.

## Conclusion

Industrial Control Systems (ICS) due to their nature are critical infrastructures for each country, as critical infrastructures are a target for would-be intruders. These systems are relatively difficult to break but not impossible. This article discusses concerns and ways to secure such infrastructures. As the evolution of information technology grows, so will the potential for breach of such systems. The security administrators must find a step forward from the intruders to secure their infrastructures. They must somehow read the intruders' thoughts and secure their systems before being attacked.

## Bibliography

1. Christos Beretas (2016). US Cyber Strategy of 2020. *Journal of Computer Engineering & Information Technology,* 2016.

2. Christos Beretas (2017). Cloud Computing and Privacy. *Journal of Electrical & Electronic Systems,* 2017.

3. Christos Beretas (2018). Security and Privacy in Data Networks. *Research in Medical & Engineering Sciences, 5*(4), 469-478.

4. Christos Beretas (2018). Internet of Things and Privacy. *Journal of Industrial Engineering and Safety, 101,* 1-12.

5. Christos Beretas (2020). Cyber Hybrid Warfare: Asymmetric threat. *Journal of Nanotechnology and Advanced Material Science, 3*(1), 1-2.

6. Christos Beretas (2020). Smart Cities and Smart Devices: The Back Door to rivacy and Data Breaches. *BIOMEDICAL: Journal of Scientific & Technical Research, 28*(1), 21221-21223.

7. https://www.researchgate.net (Industry 4.0).