UNED

INDUSTRY 4.0 CYBERSECURITY

Abstract

Industry 4.0 defines the concept of smart factories. This concept relies on many different technologies such as Internet of Things (IoT), Communication protocols, Cloud computing, Big data and Artificial Intelligence algorithms. But all these technologies need to be linked and implemented in secure way. For this reason, Cybersecurity is a key factor in designing smart factories. European agencies such as ENISA highlights the necessity of focusing on addressing the security and privacy challenges related to the evolution of industrial systems and services.

Erasmus+
Key competences for an European model of Industry 4.0
i4EU Project

Learn more about us here:
https://www.i4eu-pro.eu

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

Cybersecurity is a very important field in industry 4.0. It must always be present in the design of smart industries. From IoT devices and software used in the industrial processes to industry staff. In the last decades several industries, such as energy and financial industries, have suffered important attacks. Therefore, the creating plans and programs of study of Industry 4.0 security experts is a key factor for European Union.

Challenges

Industry 4.0 has changed work culture where people, processes and technologies have also changed:

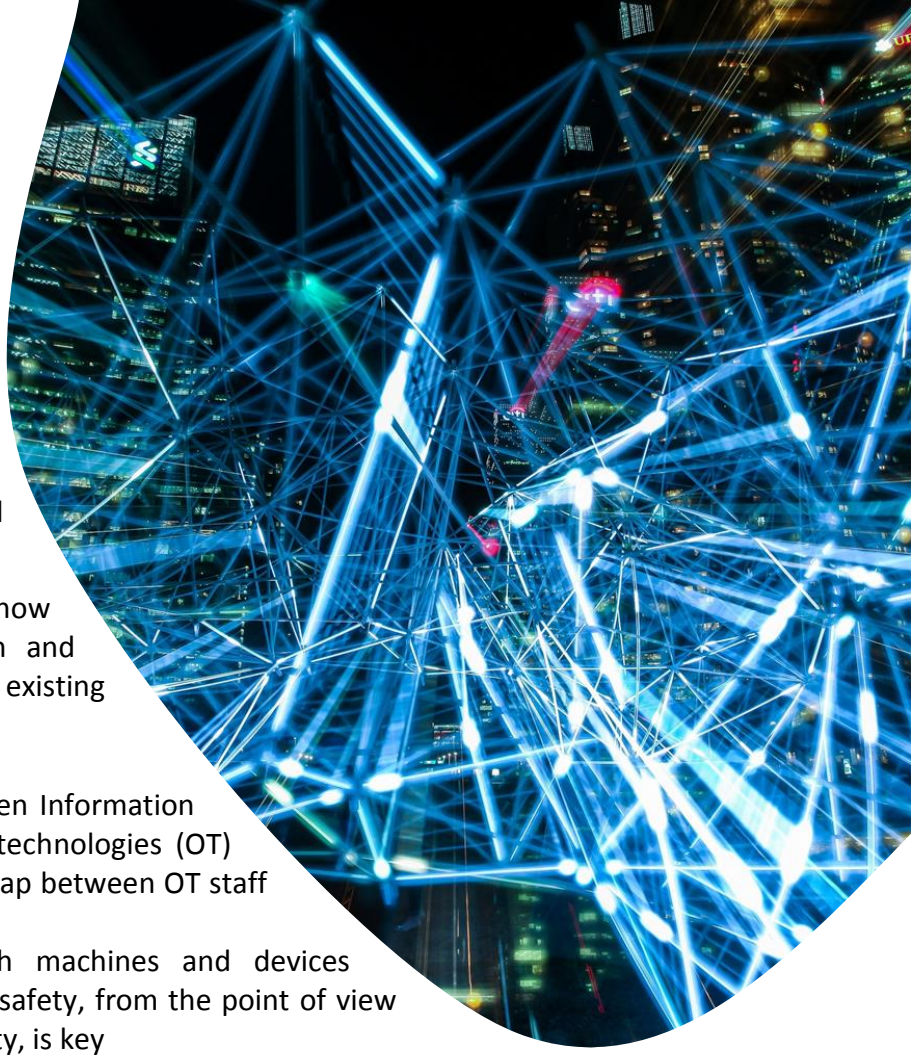
- People involved in deployments of industry 4.0 solutions usually have only knowledge of either IT (information Technologies) or OT (Operational Technologies) security, while Industry 4.0 needs both knowledge.

- Processes. There is a great number of stakeholders involved in the supply chain and in the use lifecycle of Industry 4.0, therefore apportioning liability in the aftermath of a security incident becomes challenging as currently, only general provisions of liability are applicable.

> *People, processes and technologies are key factors for the successful implementation of industry 4.0*

- Technologies. Industry 4.0 devices, platforms and frameworks to existing systems comes the issue of interoperability. In industrial environments, securing interconnectivity between diverse devices is often challenging, especially when considering devices that are long out of support.

Co-funded by the Erasmus+ Programme of the European Union



How will solve the problem?

To solve these challenges, it is necessary to foster plans and programs of study of Industry 4.0 security experts. These should cover a wide variety of challenges, such as:

- Legal Aspect. Students must know European and national legislation and case law especially where gaps in existing legislation are identified.

- Communication mechanism between Information technologies (IT) and operational technologies (OT) staff. At this moment, there are a gap between OT staff and IT staff, and it must be solved.
    - OT Staff. They work with machines and devices prevails, the importance of safety, from the point of view of physical and process safety, is key
    - IT staff. They Work with information and the confidentiality of the data is a key point.

  Therefore. Encourage cross-functional security and safety knowledge exchange between IT and OT experts respectively is really important.

- Designing and implementation of security politics. These can be classified into several categories, such as:
    - Access Control Policy. This identifies the resources that need protection and the rules in place to control access to those resources.
    - E-mail Policy. This addresses the proper use of the company e-mail system.
    - Human resources management policy.
    - Ensure that all personnel have knowledge about the rights, duties and responsibilities in relation to information security.

- Technologies. Students must learn security issues such as network security, embedded systems, OT and IT security. A working group with different experts in each field is a key factor for Industry 4.0

References

- Digital Transformation Monitor (European Comission) Digital Transformation Monitor (European Comission) https://ec.europa.eu/growth/tools-databases/dem/monitor/content/welcome
- New curricula for the fourth Industrial Revolution! (European Comission) https://ec.europa.eu/easme/en/news/new-curricula-fourth-industrial-revolution
- Industry 4.0 Cybersecurity Challenges and Recommendations (European Union Agency for Cibersecurity) https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations
- Top 5 most dangerous industrial cyberattacks https://www.stormshield.com/news/top-5-most-dangerous-industrial-cyberattacks/

This showcase has been collected in the framework of the Erasmus+ project Key competences for an European model of Industry 4.0 (pr. n° 2019-1-FR01-KA202-062965), funded by European Commission.