Industry 4.h
TECHNOLOGY SERVING PEOPLE
BY FONDATION GRENOBLE INP

CYBERSECURITY IN INDUSTRY 4.0
CONTEXT SCENARIO

ACTIVITY SUMMARY

The activity is conducted as an interactive cybersecurity training in which participants learn to secure Industrial Control Systems (ICS) through classroom instruction, simulation, and hands-on laboratory activities. Trainees configure PLC-based systems, analyse industrial communications, and explore cyber-attack and defence scenarios in a realistic cyber-physical manufacturing environment.

TEACHING APPROACH

HANDS-ON EXPERIENCE

SIMULATION BASED LEARNING

CHALLENGE BASED LEARNING

INTERACTIVE TEACHING

MATERIELS

SIMULATION SOFTWARE

PLC TRAINING PLATFORM

INDUSTRIAL NETWORK EQUIPMENT

LEARNING OBJECTIVES

Knowledge

- Explain the fundamentals of Industrial Control Systems (ICS) and industrial cybersecurity.
- Understand the differences between IT and Operational Technology (OT) environments.
- Describe common cybersecurity threats affecting cyber-physical manufacturing systems.

Technical skills

- Configure PLC-based industrial communication systems using simulation and laboratory tools.
- Analyse industrial communication protocols and network traffic.
- Apply cybersecurity principles to identify vulnerabilities and improve system resilience.

Interpesonnal skills

- Collaborate effectively during cybersecurity investigations and practical exercises.
- Develop analytical and problem-solving skills in industrial cybersecurity scenarios.
- Communicate technical findings and propose appropriate cybersecurity measures.
- Recognize the importance of cybersecurity awareness and continuous learning in Industry 4.0.

RESPONSABILITY

- The Automation Engineer can take responsibility for configuring and securing PLC-based industrial control systems.
- The Industrial Cybersecurity Engineer can take responsibility for identifying vulnerabilities and implementing appropriate cybersecurity measures.
- The Control Systems Engineer can take responsibility for monitoring industrial communications and ensuring the secure operation of cyber-physical systems.
- The Industrial Network Engineer can take responsibility for analysing communication protocols and supporting the resilience of connected manufacturing systems

CYBERSECURITY IN INDUSTRY 4.0
CONTEXT SCENARIO

SPECIFICATIONS OF THE ACTVITY

AWAKEN TRAINEES CURIOSITY

Recommended duration : 20min

Introduce the increasing cybersecurity challenges faced by modern Industrial Control Systems (ICS) and cyber-physical manufacturing systems. Present real industrial cyberattacks and discuss their consequences on production, safety, and business continuity. Explain the objectives of the training and motivate participants through realistic industrial scenarios.

RAISE AWARENESS OF THE IMPORTANCE OF CYBERSECURITY IN ENSURING SAFE, SECURE, AND RESILIENT INDUSTRIAL OPERATIONS.

CONVEY THE FUNDAMENTAL KNOWLEDGE

Recommended duration : 30 min

Introduce the fundamentals of Industrial Control Systems (ICS), PLCs, industrial communication protocols, and cybersecurity principles. Explain the differences between IT and OT environments and present the simulation and laboratory tools that will be used during the practical activities.

ENSURE THAT TRAINEES UNDERSTAND INDUSTRIAL COMMUNICATIONS, PLC OPERATION, AND THE FUNDAMENTAL PRINCIPLES OF INDUSTRIAL CYBERSECURITY.

ENABLE TRAINEES TO APPLY THE KNOWLEDGE

Recommended duration : 70 min

Participants progressively apply the acquired knowledge through simulation and laboratory activities. They configure PLCs, implement industrial communication, analyse network traffic, validate system behaviour, and identify potential cybersecurity vulnerabilities using industrial software and hardware platforms.

DEVELOP PRACTICAL SKILLS IN CONFIGURING, MONITORING, AND SECURING CYBER-PHYSICAL MANUFACTURING SYSTEMS THROUGH REALISTIC EXPERIMENTATION.

STIMULATE TRAINEES' REFLECTIONS ABOUT THE TRANING,AND FOSTER LIFELONG LEARNING AND CONTINUOUS IMPROVEMENT

Recommended duration: 15 min

Conclude the training with a collective debriefing on the practical activities. Encourage participants to reflect on the relationship between theory, simulation, and laboratory practice, discuss the cybersecurity challenges encountered, and identify opportunities for improving industrial cybersecurity practices.

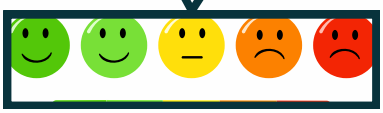
ENCOURAGE CONTINUOUS LEARNING, CRITICAL THINKING, AND COLLABORATIVE PROBLEM-SOLVING TO STRENGTHEN INDUSTRIAL CYBERSECURITY COMPETENCIES.

CYBERSECURITY IN INDUSTRY 4.0
CONTEXT SCENARIO

EVALUATION

Knowledge assessment

- Assess trainees' understanding of Industrial Control Systems and cybersecurity principles.
- Evaluate their ability to configure PLC-based industrial communication systems.
- Measure their capacity to identify cybersecurity vulnerabilities and propose appropriate countermeasures.
- Assess their ability to analyse industrial communication and apply secure operational practices.



Perception assessment

- Gather trainees' feedback on the learning experience across classroom, simulation, and laboratory environments.
- Evaluate the perceived usefulness of simulation and hands-on activities for understanding industrial cybersecurity.
- Assess participants' engagement, confidence, and collaboration throughout the training.
- Collect suggestions for improving the training content, tools, and practical activities.