Co-funded by the European Union

Didactic unit with VET students in OT and IT programmes: *Securing a smart factory*	Duration: (HOURS) 100	EQF LEVEL: 4

Learning outcomes

By the end of the activity students will be able to:

1. Describe PLC architecture and the interactions between PLCs, HMIs, sensors and the supervisory network. (Assessed: written diagram + oral explanation)
2. Perform safe reconnaissance and vulnerability analysis in a controlled OT lab; produce a prioritized pentest report. (Assessed: pentest report)
3. Design and implement monitoring (metrics, logs, dashboards) to detect anomalous behaviour and define actionable alarms. (Assessed: monitoring deliverables + detection tests)
4. Design and implement mitigations (network segmentation, access controls, PLC hardening) and verify effectiveness. (Assessed: mitigation implementation + tests)
5. Apply incident response principles: triage, containment, eradication, and recovery in an OT context. (Assessed: incident playbook + tabletop exercise)
6. Collaborate effectively in international and interdisciplinary teams and communicate technical findings to technical and non-technical stakeholders. (Assessed: peer evaluation + presentation)

TOPICS	➢ Components of an industrial plant from the point of view of cybersecurity architecture. The PURDUE model ➢ Pentesting and vulnerabilities identification and monitoring. ➢ Defence and protection of vulnerable / critical industrial infrastructure ➢ Reaction and prevention after an attack
PREVIOUS KNOWLEDGE NECESSARY	• Basic computer knowledge (network, protocol, firewall) • Basic automation architecture knowledge (PLC, industrial communications)
STRUCTURE OF THE TRAINING	• Introduction to the challenge based learning activity. Presentation of the scenarios. • Knowledge pills on IT/OT cybersecurity, PURDUE model, monitoring tools, firewalls • In between theoretical sessions, students have time to work in concrete tasks/assigments included in each of the scenarios given (online or in person) • Presentation of the common results
ASSESSMENT METHOD	• Ex-ante and ex-post evaluation questionnaire

Activity A: activity As: Activity wit assessment	Learning Outcome/s addressed	Activity Name	Activity description (Who, what and why)	Resources	Hours
A1	N/A	Introduction	The trainer will provide an introduction to the challenge based learning activity and each scenario	Challenge based learning scenarios	2 hours
A2	1	Presentation of the monitoring system and the components of the plant (which are the PLCs, which are the sensors and what they do)	The trainer will present the Purdue model using the Cyber-In interactive architecture	Cyber-In architecture, module 1 from Cyber-In MOOC	3 hours
A3	1, 6	Assignment 1 from each scneario	Students work in assigment 1 to fix previous learning	Cyber-In architecture, module 1 from Cyber-In MOOC	4 hours
A4	2,3,	Pentesting and vulnerabilities identification and monitoring	The trainer will explain what a pentest is, which kind of vulnerabilities can be found, how to rate them and which tools are available for monitoring	Cyber-In modules 3 and 5. Cyber-In knowledge pill on Zabix	3 hours
A5	2,3,6	Assingment 2 and 3 from each scenario	Students work in assigment 2 and 3 to fix previous learning	Cyber-In modules 3 and 5. Cyber-In knowledge pill on Zabix	4 hours
A6	4,5	Defence and protection	The trainer will explain which are the main protection measures to be used in an industrial environments (cero privledges policy, industrial firewalls, network segmentation)	Cyber-In modules 2 and 3	3 hours
A7	4,5,6	Assignmants 4-5/6 in each scenario	Students work in assigment 4-6 to fix to fix previous learning	Cyber-In modules 2 and 3	5 hours
A8	1-6	Attack to a virtualised industrial plant	The teacher/s needs to prepare an attack to a virtualised industrial plant using tools such as Open PLC, Linux-hacking and virtual machines	Cyber-In knowlege pills on Open PLC and Linux hacking. Virtual machines availabel in Cyber-In challenge based activity session	20 hours
A9	1-6	Detection, defence, correction	The students need to identify there has been an attack to the virtualised industrial plant they monitor, they need to act to defence the plant, create a report on what happened and put in place measures to prevent another attack	Cyber-In modules 2 and 3, knowlege pill on Zabix.	12 hours

A9	1-6	Presentation of challenge results	Students present their solution proposals for each scenario	N/A	0,5
A10	1-5	Evaluation test	Students fill an evaluation test to assess the knowledge gained about OT cybersecurity	Cyber-IN evaluation test (or any other)	