Co-funded by the European Union

**CASCADE TRAINING - ITALY WP. 3**

**Trainers: Mr. Nicola Regge, Mr. Oreste Meles (AFGP PIAMARTA)**

# 12th November 2025 - Session 1

# H. 14:30 - 16:30

### 14:30 – 14:50 | Introduction to the Cyber-IN Project

- Project objectives and expected results
- Presentation of the training modules
- Overview of the blended training experience
- Purpose and structure of the cascade training

### 14:50 – 16:00 | Introduction to Industrial Cybersecurity

- IT vs OT environments: differences and critical aspects
- What a PLC is, how it works, its evolution and vulnerabilities
- Why OT cybersecurity is critical
- Main threats to industrial systems (malware, ransomware, unauthorized access, DoS/DDoS, phishing)
- The “brain of automation”: sensors, actuators, PLC logic

**16:00 – 16:30 | Network Segmentation and Protection Mechanisms**

- What segmentation is and why it matters
- Security zones, DMZs, industrial firewalls, data diodes
- Key concepts: logical/physical isolation, ACLs, micro-segmentation
- Intrusion detection and protection systems (firewalls, authentication, antivirus)

## 26th November 2025 Session 2

## 14:30 16:30

**14:30 – 14:50 | Key Rules and Regulations on Industrial Cybersecurity**

- IEC 62443
- ISO/IEC 27001 and 27019
- NIST SP 800-82
- EU regulations: NIS2, GDPR, Cyber Resilience Act
- Obligations for institutions, operators, and the supply chain

**14:50 – 15:15 | Case Studies: Cyberattacks on Companies – practical discussion**

- WannaCry
- Stuxnet (detailed analysis: propagation and physical sabotage)
- Colonial Pipeline
- Difference in impact: *"IT protects data – OT protects lives"*

**15:15 – 15:35 | The Purdue Model**

- Levels 0–5
- Role of systems (PLC, SCADA, MES, ERP)
- Risks and best practices for segmentation between levels

**15:35 – 16:15 | Teamwork: Applying Cybersecurity in the School Context**

- How to improve OT/IT students' knowledge and skills
- Possible labs and projects (ethical hacking, OT simulations, DMZ/firewall exercises)
- Collaboration with companies, external partners, and other schools
- Opportunities to integrate cybersecurity into the curriculum
- Identification of concrete initiatives for the school
- Prioritisation of feasible activities (labs, awareness campaigns, certifications, student clubs)

Co-funded by
the European Union

**16:15 – 16:30 | Training Closure and Evaluation**

- Final Q&A
- Distribution of materials
- Completion of evaluation questionnaires (via QR codes)

**Thank you!**