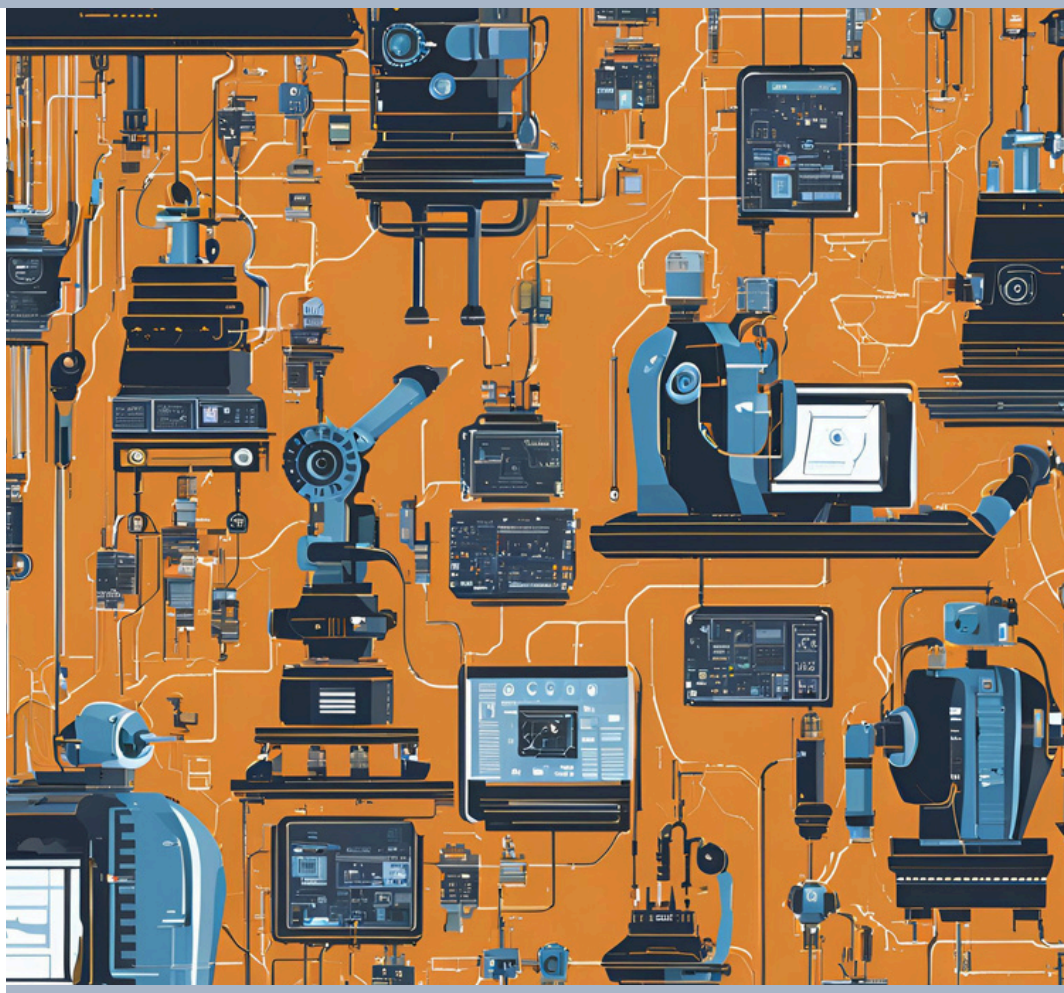
Co-funded by the European Union

CYBERSECURITY IN OT ENVIRONMENTS

SKILL GAPS AND TRAINING NEEDS

Project reference: 2023-1-NL01-KA220-VET-000153812



Prepared by:

da Vinci college

maristak
Durango ikastetxea

HETEL

ÉCOLE
ENTI CONFINDUSTRIALI LOMBARDI PER L'EDUCATION

BCS Koolitus

Roskilde Tekniske Skole

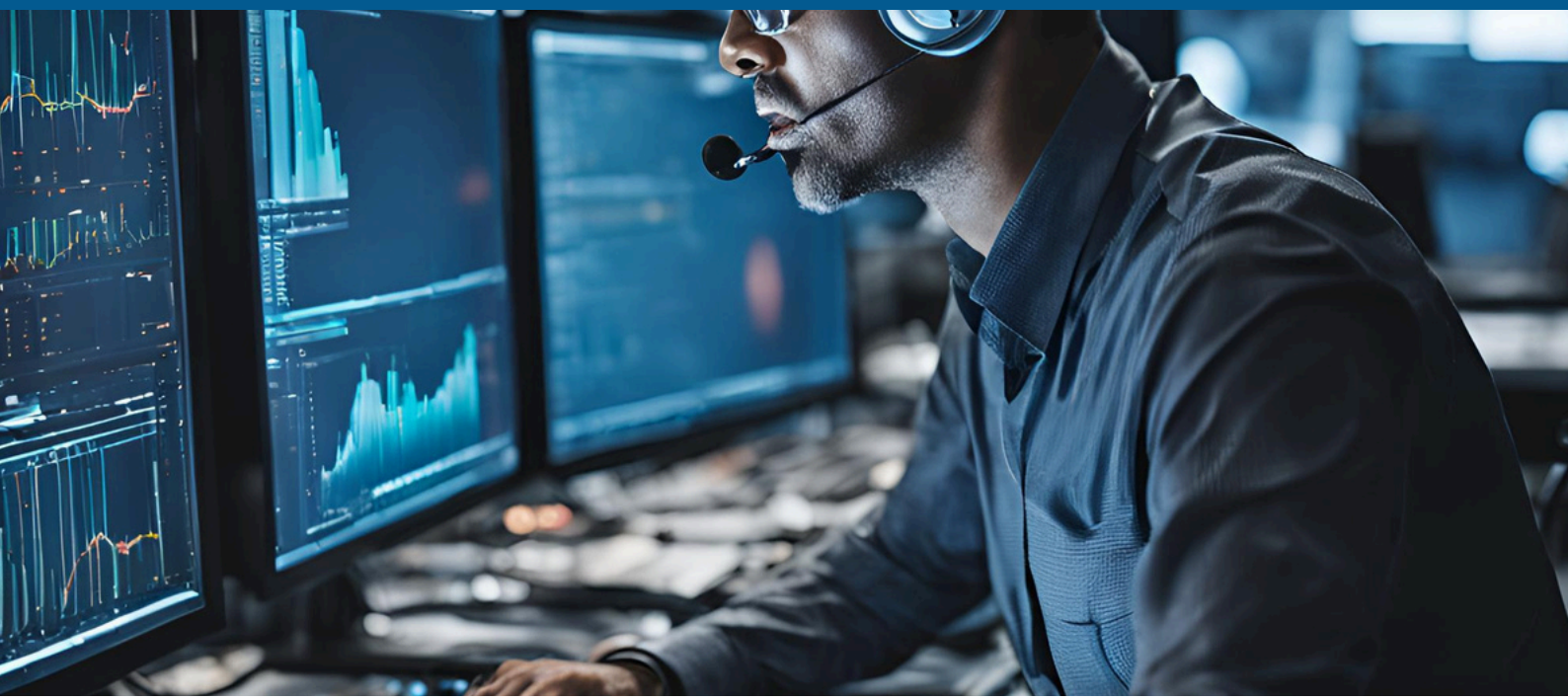
www.cyber-in.eu

Cyber-In

THIS PROJECT HAS BEEN FUNDED WITH SUPPORT FROM THE EUROPEAN COMMISSION. THIS PUBLICATION [COMMUNICATION] REFLECTS THE VIEWS ONLY OF THE AUTHOR, AND THE COMMISSION CANNOT BE HELD RESPONSIBLE FOR ANY USE WHICH MAY BE MADE OF THE INFORMATION CONTAINED THEREIN.

Table of Contents

Introduction



Cybersecurity is one of the main challenges faced by companies in the context of the Industrial Internet of Things (IoT), in which a number of smart devices associated with machines, computers and people are networked and communicate with each other.

In this connected industrial scenario, personnel need to be aware of cybersecurity issues in order to prevent or minimise the occurrence of cybersecurity incidents and corporate data breaches, and thus to make companies resilient to cyber-attacks.

Although there is growing interest in the literature in the different key elements that characterise cybersecurity management in IoT industrial contexts, little attention has been paid to the various aspects of cybersecurity awareness in the same industrial contexts.

In addition to this, Cybersecurity is not a new topic in our schools, neither in the battery of Erasmus+ projects implemented up to date. In the Erasmus+ dissemination platform there are 100 KA2 projects related to the topic. However, if we take into consideration the applications of cybersecurity to industry (and particularly to the industry 4.0 paradigm), the results reduce significantly.

Whereas industrial companies shift towards smart manufacturing and the digitalisation of machinery, data, processes and work stations with the application of facilitating technologies such as IoT, cloud computing or big data with the objective to gain efficiency in their response to continuously changing markets, the vulnerabilities in terms of cyber safety increase exponentially.

The final objective of this document was to determine which are the gaps of IT and OT professionals working in industries with a high level of automation in terms of cybersecurity so vocational schools can address those gaps when providing training to students in IT and OT programs.

To do so, we carried out interviews and focus groups in the partner countries (Netherlands, Spain, Denmark, Estonia and Italy) to get a deeper understanding of the real challenges of interconnected industrial plants in terms of cybersecurity and data protection.

The first step was to understand the challenges/weak points and needs faced by the interconnected industry in terms of cybersecurity in order to better define and detail a profile description of an OT profile with cybersecurity skills demanded by interconnected industries and an industrial IT supporter with the necessary skills to bridge the OT world.

Next we combined the feedback received from companies with an analysis of the current curricula we are already teaching in our vocational schools, identifying gaps related to cybersecurity. The result was a definition of cybersecurity skills for IT and OT professionals that can be used as a basis to develop training materials to address those gaps, materials which can be used by teachers/trainers for self-learning as well as be embedded in the current curricula of our VET programs or used by companies for internal training of their own IT and OT staff.

In the following sections we present our findings and the results of our research and analysis.

Findings from companies

Each partner carried out focus groups and/or interviews with companies in each local context (Italy, Denmark, Spain, Netherlands and Estonia).

Mixing IT and OT actors and trainers/teachers enabled us to collect information by making targeted questions in order to understand which are the cybersecurity challenges faced by interconnected industries.

Number of companies providing feedback

34 companies

Number of sectors involved

11 sectors

The objective of the focus groups and interviews was to find out main gaps detected from a technical and soft skills point of view and to draw conclusions about the need of a new profile OT/IT with upskilling/reskilling of current workers/students:

- Understand what OT companies from the sectors defined already know about cybersecurity (main concepts, business context...)
- Define the degree of awareness about the risks (sector specific weaknesses, human factor, existence of protocols and regulations...)
- Explore rules known about cybersecurity (standards and regulations applied to the specific sector)
- Explore incidents faced by other companies (case studies, simulations...)
- Understand what is the knowledge of IT cybersecurity companies and/or IT professionals, about risks faced by OT companies
- Detect knowledge, skills, awareness gaps/needs among students and workers in both fields.

For privacy reasons, we are not sharing the names of the companies interviewed, but we share the sectors they come from as well as the role of the interviewee/participant in the focus group.

COUNTRY	PARTNER	COMPANY AREA	ROLE OF THE INTERVIEWED
DK	Roskilde Tekniske Skole	Production for aviation	Infrastructure Supervisor
DK	Roskilde Tekniske Skole	water supply	Team Leader
DK	Roskilde Tekniske Skole	production of medicin	SVP Education Proffessional
DK	Roskilde Tekniske Skole	water supply	
DK	Roskilde Tekniske Skole	water supply	Operations Manager
ITA	ECOLE SCARL	Cybersecurity and consultancy	Lead Reliability & Planning
ITA	ECOLE SCARL	Electrical engineering	Strategic Planner & Automation Specialist
ITA	ECOLE SCARL	Chemicals and energy company	APC & Cybersecurity Specialist
ITA	ECOLE SCARL	Pharmaceutical chemical	CYBER SECURITY MANAGER
ITA	ECOLE SCARL	ENGINEERING, PROCUREMENT & CONSTRUCTIO	ICT Budget & Reporting Analyst
ITA	ECOLE SCARL		Account Specialist, Senior Security Engineer
EST	BCS Koolitus	Telecommunication equipment production	Cybersecurity engeneer
EST	BCS Koolitus	IT security solutions	Head of Department, IT specialist (2 people)
EST	BCS Koolitus	IT security solutions	IT specialist
EST	BCS Koolitus	Telecommunication, production	Sysadmin
EST	BCS Koolitus	Governmental Institution	Helpdesk Operations Manager
EST	BCS Koolitus	Gambling software development	IT specialist
EST	BCS Koolitus	VET College	IT specialist, teacher of IT
EST	BCS Koolitus	Wood production	IT specialists (2 people)
EST	BCS Koolitus	Food production	IT specialist
EST	BCS Koolitus	VET	IT specialist, teacher of IT
EST	BCS Koolitus	VET	Teacher of Cybersecurity, cybersecurity expert
EST	BCS Koolitus	VET	Teacher of Cybersecurity, cybersecurity expert
ES	Maristak / HETEL	IT security solutions	CEO
ES	Maristak / HETEL	Cybersecurity association	Managing Director
ES	Maristak / HETEL	Transport - Automotive	IT Manager
ES	Maristak / HETEL	Energy - Solar	Cybersecurity manager
ES	Maristak / HETEL	Energy - Wind	Cybersecurity manager
ES	Maristak / HETEL	Energy - Chemical	IT manager
ES	Maristak / HETEL	Energy - Electric equipment	Cybersecurity manager
ES	Maristak / HETEL	Transport - Aviation	Cybersecurity manager
ES	Maristak / HETEL	Transport - Machine tool	HR manager
NL	Da Vinci College	Robotics (welding)	Device manager
NL	Da Vinci College	Industrial Analytics en Machine Learing	Junior consultant smart technologies
NL	Da Vinci College	IT solutions	CEO
NL	Da Vinci College	Fiber optics/network solution	Manager
NL	Da Vinci College	Security	Support specialist

We addressed 10 questions to the companies, categorised in 3 thematic areas:

- Area 1. Understand what OT companies already know about cybersecurity.
- Area 2. Understand what is the knowledge of IT cybersecurity companies about risks faced by OT companies
- Area 3. Detect knowledge, skills, awareness gaps/needs among students and workers in both fields.

The findings in the project countries (Italy, Estonia, Spain, Denmark and Netherlands) provided a detailed overview of the challenges and opportunities in the cybersecurity landscape. Hereinafter are available the results obtained, grouped by thematic areas and questions made during the focus groups/interviews.

Thematic area 1: Cybersecurity awareness and risks in OT companies

Key Questions provided during Focus groups/interviews in this themati:

1 What are the benefits or competitive advantages of cybersecurity in your sector?

2 What kind of cybersecurity incidents or threats have you experienced and how have you managed them? What lessons have you learned from cybersecurity incidents you or other companies have experienced?

3 What level of cybersecurity training and awareness do your employees and collaborators have? What training or information actions do you carry out in this regard?

Benefits

Companies in the involved countries recognize that cybersecurity offers numerous advantages, including increased customer trust, protection of sensitive information, and ensuring operational continuity. However, there are significant differences in specific motivations and perceived benefits across different sectors and countries.

Country-specific analysis

Italy: Italian companies, particularly in the pharmaceutical sector, have seen a significant increase in cybersecurity awareness in recent years. Many large companies have implemented centralized cybersecurity functions and mandatory training programs for all employees, including suppliers. This approach has improved the protection of sensitive information and created a safer, more regulated work environment, enhancing the competitiveness of these companies.

Spain: In Spain, cybersecurity has become an essential component of business strategies, especially in regulated sectors like energy and operational manufacturing (OT). Compliance with regulations, such as the NIS2 directive, is seen as a competitive advantage that strengthens companies' positions in the market. Cybersecurity also enhances customer trust and reduces financial risks associated with data breaches and cyberattacks.

Estonia: Estonian companies recognize that a well-configured cybersecurity system increases customer trust and protects sensitive information. Reducing the risk of attacks and improving operational efficiency are significant advantages. Additionally, employee trust in their employers has increased due to solid cybersecurity measures.

Netherlands: In the Netherlands, cybersecurity is considered a key element in maintaining competitiveness, particularly in the maritime and offshore sectors. Companies that adopt advanced security standards, such as NIS2, can ensure a secure environment for their customers, improving their market position and preventing operational disruptions.

Thematic area 1: Cybersecurity awareness and risks in OT companies

Incident management and lessons learnt

Companies have reported common experiences with phishing attacks, ransomware, and issues related to outdated systems. Responses to incidents include technical improvements, stricter policies, and advanced training. Rapid response to incidents, employee training, and continuous improvement of security policies are essential to mitigate damage and prevent future attacks.

Country-specific analysis

Italy: Italian companies have faced various incidents, including phishing attacks and issues with outdated firewalls. In one case, a large pharmaceutical company discovered vulnerabilities through dark web monitoring systems. Responses to incidents emphasized the importance of a zero-trust approach and the confirmation of each transaction through authentication. Quick incident management and thorough documentation of supplier operations were identified as keys to improving security.

Spain: Cybersecurity incidents are a reality in all sectors, including government, private companies, energy, manufacturing, banking and insurance In IT cybersecurity, common incidents include vishing, spam, ransomware and phishing, while in OT, incidents can affect industrial control systems and connected devices, with threats such as denial-of-service attacks, data manipulation, OT-specific malware, unauthorised access to SCADA systems and leaks of sensitive information. Companies have learned the importance of multi-factor authentication, continuous training, and readiness to respond to attacks. The adoption of preventive measures and the improvement of security policies were crucial for effective incident management.

Estonia: Estonian companies highlighted the increasing sophistication of phishing attacks and the importance of user education to prevent incidents. Supply chain attacks and ransomware have been particularly problematic. Effective responses to incidents included technical improvements, stricter policies, and a particular focus on employee training.

Netherlands: Companies in the Netherlands have faced DDoS attacks and issues related to outdated software. Continuous training and system updates were identified as crucial factors to prevent incidents. Preparation and continuous training were considered essential to maintain a strong security posture and respond effectively to attacks.

Denmark: In Denmark, simulated attacks and brownouts are common practices to prepare companies for real situations. Risk management and preparedness for worst-case scenarios are considered fundamental to mitigate damage and ensure operational continuity.

Thematic area 1: Cybersecurity awareness and risks in OT companies

Training and awareness

Regular training, phishing simulations, and awareness programs are widely implemented. However, there are significant differences in the level of structuring and mandatory nature of training programs across different countries.

Country-specific analysis

Italy: Awareness has increased over the last 5-6 years. Industries don't manage daily with cybersecurity and networking, cause these are just the last two skills theydeveloped Cybersecurity awareness has increased due to mandatory online training cycles for all employees and suppliers in sector as pharmaceuticals and chemicals. Companies conduct continuous simulations and require employees to complete at least six hours of training before accessing corporate systems. This approach ensures that all employees maintain a high level of cybersecurity awareness and competence. Cybersecurity is today something for all employees who experience the corporate environment.

Spain: There is a significant deficit in comprehensive training, with a focus on raising awareness and integrating security measures into the company's daily culture. Training is often limited to online courses and password changes, but efforts are underway to improve employee awareness and preparedness through more structured programs.

Estonia: Cybersecurity awareness varies among Estonian companies. Some companies implement mandatory training programs and regular phishing tests, while others need improvements in communicating security policies. Continuous training and collaboration between IT departments and other departments are crucial to effectively addressing cybersecurity challenges.

Netherlands: Targeted annual training and continuous learning programs are the norm. Companies emphasize the importance of continuously updating on new threats and technologies, providing employees with the skills needed to effectively protect corporate infrastructures.

Denmark: scenario-based practical training is common, with practical security measures and regular updates provided by sector-specific CERTs. This training effectively prepares employees to handle real incidents and maintain a robust security posture.

Thematic area 2: Cybersecurity practices in IT and OT

IT and OT specifics and cybersecurity implications

OT systems are often older, less connected to the internet, and have unique operational requirements compared to IT systems, which focus more on data security. Both environments require tailored cybersecurity measures, with particular attention to real-time operations and legacy system compatibility.

Country-specific analysis

Italy: OT systems require significant investments in security updates and close collaboration with IT departments. Network segregation and secure supplier management are crucial for protecting systems from unauthorized access and vulnerabilities.

Spain: The lack of standardization in OT systems poses a significant challenge. Cybersecurity must be tailored to meet the specific needs of each system, with particular attention to regulatory compliance and risk management.

Estonia: Estonian companies often use legacy systems and isolated networks, which require network segmentation and redundant devices to maintain security. Limited internet connectivity reduces attack vectors but also makes updating and patching systems more difficult.

Denmark: In Denmark, isolated and encrypted networks are common to protect critical infrastructures. Practical security measures, such as the use of encrypted tunnels and network segmentation, are essential for protecting OT systems from unauthorized access.

Netherlands: The speed and reliability of systems are prioritized. Companies must continuously update technologies and train employees to maintain a high level of security. Network segmentation and strict access controls are common practices.

Thematic area 2: Cybersecurity practices in IT and OT

Constraints and solutions

The main constraints include financial limitations, outdated equipment, and limited internet access. Common solutions include network segmentation, strict access controls, and regular updates. Collaboration between IT and OT departments is crucial to overcome these challenges.

Country-specific analysis

Italy: Financial and legal constraints represent significant challenges for Italian companies. Supplier liability and co-development of security solutions are strategies used to improve OT system protection. Synchronization with the IT department and good internal management are crucial for maintaining a high level of security.

Spain: the obsolescence of OT systems and the lack of strict controls pose common challenges. Regulatory compliance and a risk-based approach are essential for protecting OT environments. Companies must implement tailored solutions to effectively manage the security of legacy systems..

Estonia: Estonian companies face challenges related to outdated equipment and limited internet access. Specialized training and strict access controls are recommended to improve security. Network segmentation and isolation of legacy systems are common practices to protect devices from external attacks.

Denmark: Challenges include old systems and secure communication between OT devices. Preparedness and multi-layered security are considered fundamental to mitigate damage and ensure operational continuity. Companies must implement practical security measures and regular updates to protect critical infrastructures.

Netherlands: Financial constraints and a lack of specific OT expertise represent significant challenges. Continuous training and regulatory compliance are essential to improve security. Companies must find the right balance between security and operability to maintain a high level of protection.

Thematic area 2: Cybersecurity practices in IT and OT

Criteria, priorities and impact on cybersecurity management

Ensuring continuity, quality, and efficiency through standardized procedures, regular backups, and real-time monitoring is crucial. Balancing operational needs and security requirements is fundamental for effective cybersecurity management.

Country-specific analysis

Italy: The adoption of passwordless systems and secure employee connectivity are priorities. "No shaming" policies improve cybersecurity culture and encourage employees to report incidents without fear of repercussions.

Spain: Criticality classification and impact analysis are essential for identifying critical components and implementing appropriate security measures. Network segmentation and the implementation of advanced monitoring systems are common practices for protecting OT infrastructures.

Estonia: Estonian companies adopt regular backups, user training, and compliance with international standards to maintain a strong security posture. Network segmentation and isolation of legacy systems are essential for protecting devices from external attacks.

Denmark: Multi-layered security and emergency plans are considered fundamental for ensuring operational continuity and the security of critical infrastructures. Companies implement practical security measures and regular updates to protect OT systems from unauthorized access.

Netherlands: A clear organizational structure and real-time response are essential for ensuring security and operational continuity. Flexibility in security management is crucial to address new threats and maintain a high level of protection.

Thematic area 3: Knowledge gaps and skill needs

Professional profiles and competences sought

Companies value a combination of technical skills, problem-solving abilities, and a systemic understanding of cybersecurity. Teamwork and communication skills are also crucial. This highlights the need for well-rounded professionals capable of adapting to evolving cybersecurity challenges.

Country-specific analysis

Italy: Understanding business risks and having a systemic vision are important. Technical skills in automation and IT are fundamental. Cross-functional collaboration and critical thinking are valued. Companies seek professionals who can understand risks holistically and communicate effectively with various stakeholders.

Spain: A combination of transversal competences such as communication, teamwork, problem solving and flexibility and technical competences such as SCADA, industrial firewalls and network segmentation are demanded by Spanish companies, always with a holistic understanding or the organisation and the core business.

Estonia: Being able to work across departments and technical skills to ensure the protection of legacy systems and network segmentation are at the core of the skills demanded by Estonian companies. Specialists in industrial networks management and administrators are highly desired profiles.

Denmark: Practical skills in managing critical infrastructures, internal training, and scenario-based approaches are common. Multi-layered security and preparedness are fundamental. Companies seek profiles with practical experience in managing OT system security.

Netherlands: Technical expertise in ICT and cybersecurity, knowledge of international standards, and strong communication skills are crucial. Continuous learning and adaptability are essential. Companies seek professionals with skills in cloud security and AI.

Thematic area 3: Knowledge gaps and skill needs

Specific technical skills in cybersecurity

Knowledge of SIEM, EDR, network security, and compliance with international standards is widely recognized. Critical thinking and problem-solving skills are highly valued. Continuous learning and staying updated with the latest security trends and technologies are essential for cybersecurity professionals.

Country-specific analysis

Italy: Required technical skills include security event management (SIEM), endpoint detection and response (EDR), and network security. Critical thinking and risk assessment are fundamental. Companies also seek skills in identity and access management (IAM) and security log analysis.

Spain: Required skills include vulnerability analysis, incident management, and knowledge of OT systems. Continuous training and proactive measures are emphasized. Companies also seek skills in encryption, cloud security, and network monitoring.

Estonia: Technical skills include familiarity with SIEM, EDR, and network security. Continuous learning and adaptability are essential to address new threats. Companies also seek skills in identity management, firewall configuration, and vulnerability analysis.

Denmark: Practical skills in managing critical infrastructures, network segmentation, and practical security measures are valued. Preparedness and multi-layered security are fundamental. Companies also seek skills in security log management and incident response.

Netherlands: Required skills include network security, cloud computing, and AI. Compliance with regulations and continuous learning are essential to maintain a high level of security. Companies also seek skills in security data analysis, identity management, and protection of sensitive information.

Thematic area 3: Knowledge gaps and skill needs

Standards and certifications

Certifications such as CISSP, ISO 27001, and other industry standards are widely recognized and recommended. Practical experience and continuous learning are equally important. Certifications provide a benchmark for skills and knowledge, but practical experience and continuous learning are essential for maintaining high cybersecurity competence.

Country-specific analysis

Italy: Recommended certifications include CISSP, ISO 27001, and internal training programs. Emphasis is placed on continuous learning and adaptability. Companies also seek certifications in industrial systems security and identity management.

Spain: Certifications include CISSP, CISM, CEH, and ISO 27001. The importance of compliance with new regulations like NIS2 is emphasized. Companies also seek certifications in incident management and cloud security.

Estonia: Required certifications include CISSP, GSEC, ISO 27001, and local standards like E-ITS. Continuous training and phishing tests are common practices. Companies also seek certifications in identity management and incident response.

Denmark: Practical certifications like CompTIA Security+ are valued, along with internal training. Scenario-based training is fundamental. Companies also seek certifications in identity management and critical infrastructure security.

Netherlands: Required certifications include ISO 27001, NIS2, and other industry standards. Practical experience and adaptability are emphasized. Companies also seek certifications in cloud security and incident management.

Thematic area 3: Knowledge gaps and skill needs

Emerging areas within cybersecurity

Cloud security, AI-driven security, and IoT security are identified as growing areas of demand. The rapid evolution of technology requires cybersecurity professionals to continuously update their skills and adapt to new challenges.

Country-specific analysis

Italy: Focus is on systemic thinking, cloud security, and AI-driven security. Team collaboration and continuous training are essential to address new threats. Companies seek skills in security data analysis and identity management.

Spain: AI regulation and IoT security are emerging areas of expertise. Integrating AI and managing data in the cloud are considered crucial for security. Companies seek skills in encryption and protection of sensitive information.

Estonia: The dual role of AI in cybersecurity, cloud security, and regulatory compliance are growing areas of demand. Continuous training and adaptability are essential to address new threats. Companies seek skills in security data analysis and identity management.

Denmark: AI-driven security and IoT security are growing areas of demand. Multi-layered security and preparedness are fundamental to mitigate risks. Companies seek skills in identity management and protection of sensitive information.

Netherlands: Cloud security, AI-driven security, and IoT security are identified as emerging areas. Compliance with regulations and continuous learning are essential to maintain a high level of security. Companies seek skills in security data analysis and identity management.

Summary of findings

Thematic Area 1: Cybersecurity Awareness and Risks in OT Companies

Key findings. To improve cybersecurity: increase awareness, updated training, rapid incident response and continuous revision and improvement of security policies.

AWARENESS, TRAINING AND SECURITY POLICIES ARE ESSENTIAL

Benefits from enhanced cybersecurity: Enhanced customer trust, protection of sensitive information, operational continuity, increased competitiveness, regulatory compliance and operational efficiency.

Challenges: skill gaps, low awareness, management of legacy systems while maintaining real-time operational security.

Good practices: network segmentation, strict access controls and regular and system updates, collaboration between OT and IT departments.

Summary of findings

Thematic Area 2: Cybersecurity practices in IT and OT

Key findings: Tailored cybersecurity for OT environments, ensuring continuity, quality and efficiency and real-time monitoring are crucial.

TAILORED CYBERSECURITY AND NETWORK SEGMENTATION ARE KEY IN OT ENVIRONMENTS

Challenges: financial limitations, outdated equipment, limited internet access and lack of standardization.

Good practices: network segmentation, secure supplier management, multi-layered security measures, scenario-based practical training and continuous system updates.

Recommendations: Invest in specialised training and empower IT specialists to address OT specific challenges. Promote collaboration between IT and OT departments and ensure a holistic security approach

Summary of findings

Thematic Area 3: Knowledge gaps and skill needs

Key findings: A combination of technical skills, problem-solving abilities, and a systemic understanding of cybersecurity is crucial.

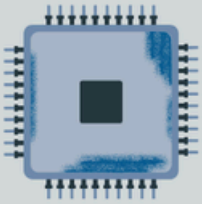
CONTINUOUS LEARNING AND A HOLISTIC APPROACH ARE ESSENTIAL

Skills demand: Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and network security. Companies also valued competencies in vulnerability analysis, incident management, and compliance with international standards. Practical experience in managing critical infrastructures and familiarity with both IT and OT systems were particularly valued.

Certifications: Certifications such as Certified Information Systems Security Professional (CISSP), ISO 27001, and other industry standards were widely recognized and recommended. These certifications provide a benchmark for the skills and knowledge required in cybersecurity roles.

Emergent areas of expertise: Cloud security, AI-driven security and IoT security.

Cybersecurity weak points in companies



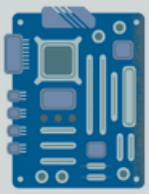
- Outdated firewalls
- Vulnerable identification systems
- Integration issues
- Lack or weak security policies
- Deficit in a comprehensive approach to cybersecurity risks
- Lack of standardization in OT systems
- Financial constraints
- Lack of specific OT expertise

Recommendations to improve cybersercurity in OT environments

- Continuous training of workers
- System updates
- Regular phishing tests / penetration tests
- Effective communication of security policy in the company
- Network segmentation and encryption
- Secure supplier management
- Regular backups
- Just in time monitoring
- Identification of critical components
- Comply with international standards
- Count with emergency plans
- Scenario based training

Skills demand for IT profiles

- Cybersecurity elements in an industrial plant
- Application of cybersecurity activities in operations and maintenance, according to the company´s security policy.
- Detection of anomalies in industrial control systems using monitoring tools and analysis procedures.



Skills demand for OT profiles

- Cloud security and AI
- Security Event Management (SIEM) and Endpoint Detection and Response (EDR)
- Network monitoring
- Security log management

Skills demand for both IT and OT profiles

- Understanding business risks and have a systematic vision
- Effective communication across profiles and departments regarding cybersecurity issues (policy, vulnerability detection, incidents...)
- International standards and regulations applied to the sector (with different proficiency levels of knowledge for IT and OT professionals). For example, CISSP, ISO 27001, NIS2.
- Understanding of the most frequent critical cybersecurity risks and their consequences/impact on the company (in terms of safety at work, money loses, environmental impact...)
- Critical thinking, problem solving, team collaboration, and continuous learning

Review of current IT and OT VET curricula

The focus groups and interviews carried out by the partners gave us an understanding of which are the weak points regarding cybersecurity in industrial automated environments. The feedback received also included some key elements to improve cybersecurity and which are the necessary skills in IT and OT profiles to implement them. Analysing the current vocational programmes that are being currently taught in the different partner countries (Netherlands, Spain, Denmark, Italy and Estonia) we were able to identify concrete gaps in relation to those cybersecurity skills demanded by companies.

As there are different vocational programmes related to IT and OT, though with different denominations in the partner countries, we focused our analysis on 2 profiles:

- For IT, the profile is that of a Technician in Network Management and Administration, i.e., the professional who plans and implements the network infrastructure in an organisation, chooses the appropriate hardware and software components, configures the network devices and protocols and coordinates the installation of the network equipment and cables, troubleshoots any issues that arise, and documents the network configuration and topology.

- For OT, the profile is that of a Technician in Automation and Industrial Robotics, i.e., the professional who works in companies related to automatic industrial systems, in the areas of design, assembly and maintenance of industrial automation systems.

Hereinafter, when we mention IT/OT profiles, we are referring particularly to this type of technicians.

For the IT profile, we have analysed the certificates described in the table below. After going through the contents and the learning outcome already covered by current curricula in the project countries, we have identified those gaps related to cybersecurity in interconnected industrial environments, based on findings from companies.

Country	Translated title of the training programme	Duration of the programme and amount of hours	EQF level	Brief explanation of the professional fields of activity
Netherlands	ICT system engineer	3 academic years (2.500 hours)	4	An ICT System Engineer at MBO Level 4 (BOL pathway) specializes in designing, implementing, managing, and maintaining IT infrastructures within organizations. They ensure that networks, servers, and operating systems run smoothly, supporting various aspects of an organization's technology needs.
Spain	Higher Technician in Computer Network Systems Management	2 academic years (2.000 hours)	5	The holder of this diploma will have acquired the general competence with regard to: Configuring, administrating and maintaining computer systems, guaranteeing system functionality, integrity of resources and services, with the required quality and complying with the current legislation.
Estonia	Information and Communication Technology level 4	2 years (if accessing from secondary education)	5	An IT systems specialist develops and manages an organization's IT infrastructure, providing modern technical solutions for comprehensive systems.
Italy	Higher Technician for IT Infrastructures, Network, Cloud and Virtualization- ITS Network and Cloud Specialist	2 years (2.000 hours)	5	This professional is able to manage, understand and design security systems for infrastructures, integrating data protection compliance rules with the various business needs.

The **ICT system engineer certificate in the Netherlands** is structured in 5 competence areas. Comparing the learning outcomes already covered by the current curriculum with the demands from industrial companies in terms of cybersecurity, below we find the skill gaps detected in each of those areas.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Supports users/requesters/clients	• Has a basic understanding of the structure of OT environments • Understands the importance of IT and OT integration - including the key differences and potential security challenges between IT and OT environments. • Can communicate with OT professionals and make the translation between the needs of OT and IT.
Installs and manages the infrastructure	• Has knowledge of OT-specific protocols and networks, such as Modbus (example). • Has knowledge and understands the structure and components of OT systems such as SCADA systems, PLCs (Programmable Logic Controllers), and DCS (Distributed Control Systems) • Understands network segmentation for OT environments, knowledge of network design principles that isolate OT systems from IT networks to minimize risks.
Manages applications	• Has knowledge of patch management for OT systems understanding unique challenges of updating OT devices, considering factors like system downtime and compatibility. • Has knowledge of used applications for OT systems
Develops digital information systems (database management)	• Has knowledge of basic scripts using in OT environment and vulnerabilities. • Has knowledge of different data platforms to secure (big) data.
Security checks	• Has knowledge of the potential vulnerabilities associated with OT systems such as SCADA • Can perform risk assessments specific to OT environments to detect the basic vulnerabilities in OT systems • Has knowledge of potential vulnerabilities associated with OT hardware such as PLC's • Has knowledge of various regulations and legislation related to OT cybersecurity, such as NIS2, iso 27001 • Has specific knowledge of hardware and software focused on OT cybersecurity to secure systems and networks

In **Spain, the curriculum of Higher Technician in Computer Network Systems Management** is structured in modules. For each of the technical ones, we have identified the gaps related to industrial cybersecurity.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Operating Systems Implementation	• Knows what a SCADA system for a production plant is.
Network Planning and Management	• Designs and configures network segmentation in a production plant, ensuring the implementation of cybersecurity measures to protect critical infrastructure and limit access to sensitive systems. • Knows industrial protocols such as Modbus and OPC-UA
Hardware Fundamentals	• Implements physical (authentication, camera) and logical (antivirus, anti-malware) security policies to protect critical OT devices, ensuring the integrity and availability of industrial systems. • Knows what is a PLC, its feautures and general functions
Database management	• Designs and executes secure SQL queries, implementing input sanitization techniques to prevent SQL injection attacks.
Markup Language and Information Management Systems	• Implements data validation measures to prevent code injections in XML documents, data encryption in the exchange of sensitive information, and configure control access permissions to prevent Cross-Site Scripting (XSS) attacks in HTML interfaces
Operating Systems Management	• Implements Active Directory to control access to industrial systems, enforces security policies, and performs auditing and monitoring to protect against security threats. • Configures cloud services, such as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), to improve the efficiency, security and scalability of industrial systems.
Network Services and Internet	• Implements industrial wireless networks applying industry standards. • Manages critical network services in industrial environments, such as SCADA servers, distributed control systems (DCS), and industrial sensor networks. Implements intrusion detection systems (IDS) and network segmentation to protect critical systems against unauthorized access.
Web Applications Implementation	• Configures web applications used in industrial environments, ensuring that appropriate security measures such as authentication, data encryption, and protection against common vulnerabilities such as SQL injections and Cross-Site Scripting (XSS) attacks are implemented.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Database Management Systems Administration	• Implements cybersecurity measures with MES systems, controlling access to data, continuously monitoring and ensuring the availability of distributed databases.
Safety and High Availability	• Configures specific firewalls to protect industrial networks against unauthorized access and cyber-attacks. • Knows and applies cybersecurity regulations (NIS2) and standards (IEC 62443, NIST SP 800-82, ISO 27001) specific to industrial environments. • Develops, implements and manages security policies in OT environments. • Knows echniques to identify, preserve, analyse and present evidence in case of security incidents, using forensic analysis tools (Autopsy) to perform forensic investigations in industrial systems. • Implements virtualization solutions to improve the security and management of industrial systems, enabling rapid response to incidents. • Configures high availability systems to ensure operational continuity of critical industrial systems, minimizing downtime in case of attacks.
Transversal skills related to cybersecurity in interconnected industrial environments	• Understands business operations and critical risks, having a systemic/holistic vision of the different areas/departments and the interactions among them. • Understands the most frequent critical cybersecurity risks and their consequences/impact on the company (in terms of safety at work, money loses, environmental impact...) • Communicates effectively across the organisation´s profiles, departments, regarding cybersecurity issues (policy, vulnerability detection, incidents...) • Collaborates with the OT profiles in the organisation to implement cybersecurity activities in the operation and maintenance of the industrial plant. • Makes decisions in critical situations. • Plans tasks. • Escales incidences.

Estonian studies for Information and Communication Technology offer different alternatives of specialization based on optional subjects. The curriculum is structured in ECVET credits and offer great modularization. However, even itineraries specialised in cybersecurity present gaps in terms of industrial cybersecurity. Those are the ones we have detected attending to 7 areas of competence:

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Information Security Management	• Understanding frameworks like NIST Cybersecurity Framework, ISO 27001, and CIS Controls. • Creating and maintaining documentation according to standards like E-ITS and ISO 27002.
Business Continuity Management	• Understanding and addressing cloud-specific security risks is essential. • Understanding data privacy regulations (e.g., GDPR, CCPA) and implementing measures to protect sensitive data.
Service Delivery	• Identifying, assessing, and mitigating vulnerabilities in systems and applications. • Developing and implementing incident response plans to effectively handle security breaches. • Developing and delivering security awareness training to employees to improve their understanding of security threats and best practices. • Understanding cloud security models (IaaS, PaaS, SaaS) and implementing measures to protect data and applications in the cloud. • Configuring firewalls, intrusion detection systems, and other network security controls to protect against unauthorized access.
Securing IT solutions	• Understanding of user rights and permissions within security systems. • Familiarity with specific technologies, such as MS Security. • Knowledge of relevant laws and standards (e.g., E-ITS, ISO). • Ability to configure and understand security policies. • Knowledge of firewall rules, log analysis, and management. • Expertise in various cybersecurity tools, including IDS, firewalls, and SIEM systems. • Understanding and implementing application security best practices to protect applications from vulnerabilities.
Transversal competences	• Analytical and problem-solving skills: The ability to analyse complex security incidents and develop effective solutions. • Communication skills: Strong communication skills to collaborate with teams, stakeholders, and external parties. • Ethical hacking knowledge: A deep understanding of ethical hacking techniques to identify vulnerabilities and improve security posture. • Continuous learning: A commitment to staying updated with the latest cybersecurity trends, threats, and best practices.

VET curricula in Italy are designed by the regions and may be different, even quite different, among them. Futhermore, curricula may even vary from school to school, especiallyl in professions related to technology and digitalization. In the case of **Italy**, we chose to analyse the curricula for the **Higher Technician for IT Infrastructures, Network, Cloud and Virtualization- ITS Network and Cloud Specialist,** for being the closest to the others analysed by the partners.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Hardware and software installation	• Training on specific methods for maintaining security during hardware and software installation, especially in mixed IT/OT environments. • Ensuring compatibility while maintaining information security. • Identifying and mitigating vulnerabilities that may arise during system integration. • Addressing the risks introduced by integrating new technologies with legacy systems, particularly those vulnerable to common threats like phishing or outdated components. • Improving awareness and response to common attack vectors during component installation and configuration.
Computer architecture	• Identifying and addressing potential vulnerabilities in hardware/software design. • Implementing security features that adapt with both business and technological changes. • Securing new architectural changes to mitigate the risk of cyber threats. • Emphasizing secure design principles for scalable and interoperable architectures. • Strengthening the systemic understanding of cybersecurity needs, ensuring that scalability and interoperability are aligned with robust security frameworks. • Incorporating practical training in vulnerability identification and assessment during architecture design. • Enhancing training on regulatory compliance and applying cybersecurity standards during the architecture phase.
IT systems administration	• Understanding secure practices for installing and upgrading software. • Implementing secure procedures for configuring system updates. • Developing awareness of the risks related to outdated software and updates. • Emphasis on secure software update practices, including patch management that addresses vulnerabilities in both IT and OT systems. • Practical training on dealing with outdated OT systems and their cybersecurity challenges, such as maintaining security while upgrading old technologies. • Addressing skills gaps in specific security tools, like Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) systems.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
System maintenance	• Applying secure methods during system repairs to prevent vulnerabilities. • Recognizing cybersecurity threats while executing maintenance tasks. • Responding to incidents related to system performance vulnerabilities; Handle and manage incidents holistically while maintaining high customer satisfaction. • Secure management of repair activities, particularly regarding legacy systems. • Cybersecurity during physical repair activities and aligning these with defined procedures to prevent unauthorized access.
IT operations	• Advanced cybersecurity threat detection and mitigation techniques • Disaster recovery plans with cybersecurity measures. • Real-time responses to threats, ensuring operational continuity. • Secure backups, including managing security risks during data storage and recovery. • Addressing challenges in ensuring continuity, quality, and efficiency in OT systems while maintaining cybersecurity standards.
Automation	• Secure scripting practices to ensure management automation doesn't introduce vulnerabilities. • Understanding potential vulnerabilities in automation tools and procedures. • Cybersecurity related to automation tools, including vulnerabilities inherent to older or legacy OT systems • Automating cybersecurity checks for compliance and system integrity. • Collaboration with OT departments to address cybersecurity in automation comprehensively.
Cloud computing	• Applying cloud-specific cybersecurity measures to secure virtual environments. • Securing data privacy in cloud environments. • Decentralized networking security, particularly for OT environments with unique operational requirements. • AI-driven security, and IoT security. • Understanding of multi-layered security measures, particularly those aimed at managing third-party cloud services securely
Key Performance Indicators (KPI) definition and management	• Security-focused KPIs to assess and enhance the cybersecurity posture of IT and OT environments • Analysing data to identify cybersecurity gaps in system performance. • Incorporating risk-based KPIs that consider legacy systems and their potential vulnerabilities. • Ensuring that KPIs reflect evolving cybersecurity threats, such as ransomware and phishing attacks, and that they are used to drive proactive security improvements. • Interpreting KPI data to enhance decision-making regarding cybersecurity measures and priorities.

We have done the same analytical exercise with VET curricula related to professionals fit to work in industrial environments with a high level of digitalization. In this case, we have identified 2 main profiles: mechatronics and industrial automation. Each partner has analysed the curriculum related to one of them to identify gaps related in cybersecurity.

Country	Translated title of the training programme	Duration of the programme and amount of hours	EQF level	Brief explanation of the professional fields of activity
Netherlands	Technicus mechatronica	3 academic years (2.500 hours)	4	A "Technicus Mechatronica" at MBO Level 4 (BOL pathway) specializes in designing, constructing, testing, and maintaining mechatronic systems that combine mechanical, electrical, and computer-based technologies. Their work spans across various industries, including manufacturing, automation, robotics, and high-tech machinery
Spain	Higher Technician in Industrial Automation and Robotics	2 academic years (2.000 hours)	5	The holder of this diploma will have acquired the General Competence with regard to: Developing and managing projects of assembly and maintenance of automatic installations of measurement, regulation and processes control in industrial systems, as well as and supervising or assembling, maintaining and implementing these systems, respecting criteria of quality, safety and respect for the environment as well as design.
Estonia	Automatician	2 years (if accessing from secondary education)	5	The aim of the study is to acquire competences that enables them to work as a skilled worker in companies specializing in either production automation or building automation.
Italy	ITS Digital Solution 4.0 Specialist for the digital transition - ITS Industrial Digital Transformation Specialist	2 years (2.000 hours)	5	The IDT Specialists are IT professionals who develop customised integrated solutions to guide companies towards digitisation, creating cyber-physical environments that optimise data management.

In the curriculum delivered in the **Netherlands for "Technicus Mechatronica MBO 4**, there are 3 main competence areas. Although the curriculum provides a good combination of IT and OT knowledge and skills, we have still detected big gaps related to cybersecurity.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Manufacturing mechatronic products	• Has fundamental knowledge of IoT (Internet of Things), understanding how IoT is integrated into mechatronic systems for remote monitoring, control, and data collection • Has a basic knowledge of IT within an industrial environment and understands the relevant IT aspects involved. • Has knowledge of awareness to secure developments • Has knowledge to secure the infra structure of machine and machine learning
Installation and modification of mechatronic products and/or systems	• Has basic cybersecurity knowledge for industrial environments, • Knows the basic common cybersecurity risks in industrial environments • Basic knowledge of networking and connectivity, understanding the fundamentals of troubleshooting network connections • Ability to oversee risks to use/install tools • Awareness of possible threats within programs or tools to be used
Guidance and management of the work process	• Can use remote monitoring and diagnostic tools that allow remote diagnostics, monitoring, and maintenance of mechatronic equipment. • Can communicate with IT specialists to work in a problem-solving manner • Has knowledge of data protection • Has knowledge or understands cybersecurity threats, such as phishing, malware, or social engineering tactics.

In **Spain, we have analysed the profile of a Higher Technician in Industrial Automation and Robotics**, which is the one most demanded by companies in our context to merge with IT skills related to cybersecurity. The Spanish Goverment has even created a specialization course on cybersecurity in OT environments, accessible to those already in posession of the certificate of HT in Industrial Automation and Robotics (more information in the Europass supplement:

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Electrical, Pneumatic and Hydraulic Systems	• Is aware of the need to change default passwords for devices such as relays or pneumatic controllers to protect access to equipment.
Programmable Sequential Systems	• Implements password access controls on sequential control systems to ensure that only authorised personnel can modify control logic.
Measurement and Control Systems	• Monitors and records sensor readings so that anomalous behaviour or data tampering can be identified in order to detect potential security problems.
Power systems	• Knows the importance of changing the default credentials of network-connected devices such as inverters or UPS systems, a simple but crucial practice to prevent unauthorised access
Technical documentation	• Includes change history in the technical documentation, recording who modified each section and when, which helps prevent and detect unauthorised alterations.
Industrial computing	• Installs and configures anti-virus and firewalls on computer systems controlling production, as a simple way to protect systems against malware.
Advanced programmable systems	• Blocks remote access to PLCs when it is not necessary, as a basic measure to protect against unauthorised access.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Industrial Robotics	• Sets up access lists on industrial robots to define which users can modify programs or control the robot, reducing the risk of unwanted manipulation.
Industrial communication	• Understands the main vulnerabilities related to cloud computing (misconfiguration, insider threats, data loss and leakage and insecure interfaces and APIs) and which are the methods used by hackers to make use of them (phishing, software bugs, DoS attacks, Social engineering, ransomware and malware). • Knows methods and tools to protect vulnerabilities related to cloud computing, in line with the organization's security policy. • Knows the incident response plan, part of the SIEM solution implemented by the organization. • Interprets and detects anomalies based on the data provided by the MES (Manufacturing Execution Systems) and the HMI systems. • Sets up basic encryption in data transmission, e.g. by using VPNs or secure protocols to protect communications between industrial devices.
Integration of Industrial Automation	• Takes into account the existing risks when planning and installing an automatic system, identifying when a EDR system is needed and which one to choose. • Knows the International standards and regulations applied to the sector, (for example, CISSP, ISO 27001, NIS2) and, in particular, the standard ISA/IEC 62443, specially relevant for industrial automation. • Applies security log management when planning and installing an automatic system. • Is aware of ICS (industrial control systems, such as SCADA) and knows the different components of an OT network and how they are interconnected. • Network segmentation: create diagrams isolating critical automation networks from the rest of the company's networks.
Transversal skills related to cybersecurity in interconnected industrial environments	• Understands business risks and has a systemic/holistic vision of the different areas/departments and the interactions among them. • High level of awareness of cyber risks affecting OT systems, knowing sites such as shodan.io and its section dedicated to ICS or MITREATT&CKforICS1 to assess the number of threats to which these systems are exposed. • Communicates effectively across profiles, departments, regarding cybersecurity issues (policy, vulnerability detection, incidents...) • Awareness: identification of common threats in industrial environments. • Troubleshooting: detecting and correcting security flaws. • Risk management: risk assessment: identifying potential vulnerabilities. • Effective communication: explaining basic security best practices to a non-technical audience (such as operators). • Responsibility and professional ethics: analyse security breaches that can affect individuals and businesses. • Autonomy and continuous learning: keeping up to date with the latest trends in industrial cybersecurity.

After going through different profiles in **Estonia** we have selected the curriculum for "Automatician", which is very similar in content to the Spanish curriculum, although structured in a different way, with a combination of general studies and technical studies. For the analysis, we have focused only on the technical part. Gaps related to industrial cybersecurity are very similar to the ones detected in the Spanish curriculum.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Operation of automation equipment and systems	• ICS architectures: Familiarize yourself with common ICS architectures, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs). • Industrial communication protocols: Understand protocols like Modbus, Profibus, Ethernet/IP, and OPC UA, and their security implications. • OT devices: Be aware of the unique vulnerabilities of OT devices, such as sensors, actuators, and controllers.
Installation of automation equipment and systems	• Network segmentation: Implement network segmentation to isolate OT networks from corporate IT networks and reduce the attack surface. • Firewall configuration: Configure firewalls to restrict access to OT networks and devices. • Patch management: Regularly update OT devices and software with security patches. • Access control: Implement strong access controls to limit who can access OT systems and devices. • Security monitoring: Use security monitoring tools to detect and respond to anomalous activity on OT networks.
Basic knowledge of automation	• Industrial espionage: Understand the risks of unauthorized access to OT systems for purposes of stealing intellectual property or disrupting operations. • Sabotage: Be aware of threats from malicious actors who aim to damage or disrupt critical infrastructure. • Supply chain attacks: Understand the risks of compromised hardware or software components.
Fundamentals of electrical engineering and electronics	• Knows the importance of changing the default credentials of network-connected devices such as inverters or UPS systems, a simple but crucial practice to prevent unauthorised access. • Password control and updating.
Transversal skills	• Professional update on industrial control system hacking: Stay informed about the latest techniques used by attackers to target ICS. • Artificial intelligence and machine learning to improve OT security, such as for anomaly detection and predictive maintenance.

The curriculum analysed in the case of **Italy** is with no doubt the one which offers the most "hybrid" programme between IT and OT knowledge and skills of those explored by the partnership at EQF levels 4-5 in our respective countries. While it provides a good combination, we have still spotted several gaps in terms of cybersecurity.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Digital enterprise ipmlementation	• Data integrity, confidentiality, and threat detection. • Security standards and protocols in IT systems. • Scenario-based practical training and simulations to improve incident response.
Coding and testing	• Secure coding practices to prevent vulnerabilities. • Threat modelling as part of software development. • Vulnerability analysis, SIEM, and EDR systems to enhance coding security • Secure debugging methodologies to identify and mitigate security risks
Applications design and development	• Secure communication between industrial automation devices. • Vulnerabilities specific to real-time control systems. • Risk mitigation in automation networks.
IoT solutions design and implementation	• Secure network architectures for IT-OT integration. • Segmentation techniques to reduce security risks. • Legacy systems and real-time operational security. • OT-specific threat mitigation and incident response
Monitoring technology	• Cybersecurity impact of integrating new technologies. • Vulnerabilities identification introduced by emerging technologies. • Security validation before implementing new trends. • Cloud security, AI-driven security, and IoT security as emerging areas of demand.
Strategic decision making	• Incorporate cybersecurity considerations into strategic ICT planning. • Focus on data protection measures for customer-oriented processes. • Align ICT strategies with industry cybersecurity standards and compliance. • Developing cybersecurity frameworks that enhance customer trust and competitive advantage.
Data management	• Data protection during collection, analysis, and storage. • Data management in secure cloud and AI driven security. • Encryption techniques for data integrity. • Secure AI model training practices to prevent data leaks.

Competence areas	Gaps related to cybersecurity in interconnected industrial environments
Customer´s management	• Cybersecurity risk assessment as part of customer consultancy. • Secure supplier management and cybersecurity standards. • Resilient and secure technology solutions. • Customer security needs analysis for tailored advice on technology alternatives. • Incident management.
Digital transformation	• Cybersecurity risk management during digital transformation initiatives. • Standardized procedures, backups, and real-time monitoring for project continuity. • Secure communication and system integrity during changes. • Securing digital assets throughout the transformation lifecycle.
Project management	• Cybersecurity risk management in project planning. • Secure handling of critical project milestones involving IT-OT convergence. • Secure communication and coordination within cross-functional teams. • Regulatory compliance and risk-based approach to manage cybersecurity. • Cybersecurity KPIs such as incident frequency and system vulnerabilities. • Reporting of cybersecurity measures. • Performance evaluation according to cybersecurity standards.

Key findings

Both IT and OT VET programmes analysed are similar in all project countries, confirming the feedback received from companies during the focus groups, disregarding the sector they operate.

At the EQF levels analysed, we have seen that vocational programmes in Estonia and Italy offer a wider range of specialisation and mix of IT and OT contents, but still overlooking specific cybersecurity skills in industrial environments.

Next steps

After analysing the different VET programmes related to IT (network management) and OT (industrial automation and digitalization), we have classified the gaps in three groups of skills necessary for IT and OT workers in order to work in cybersecure industrial environments:

TECHNICAL COMPETENCES

Those which are necessary to carry out their regular work, including technical cybersecurity competences according to their profile and their role in the organisation.

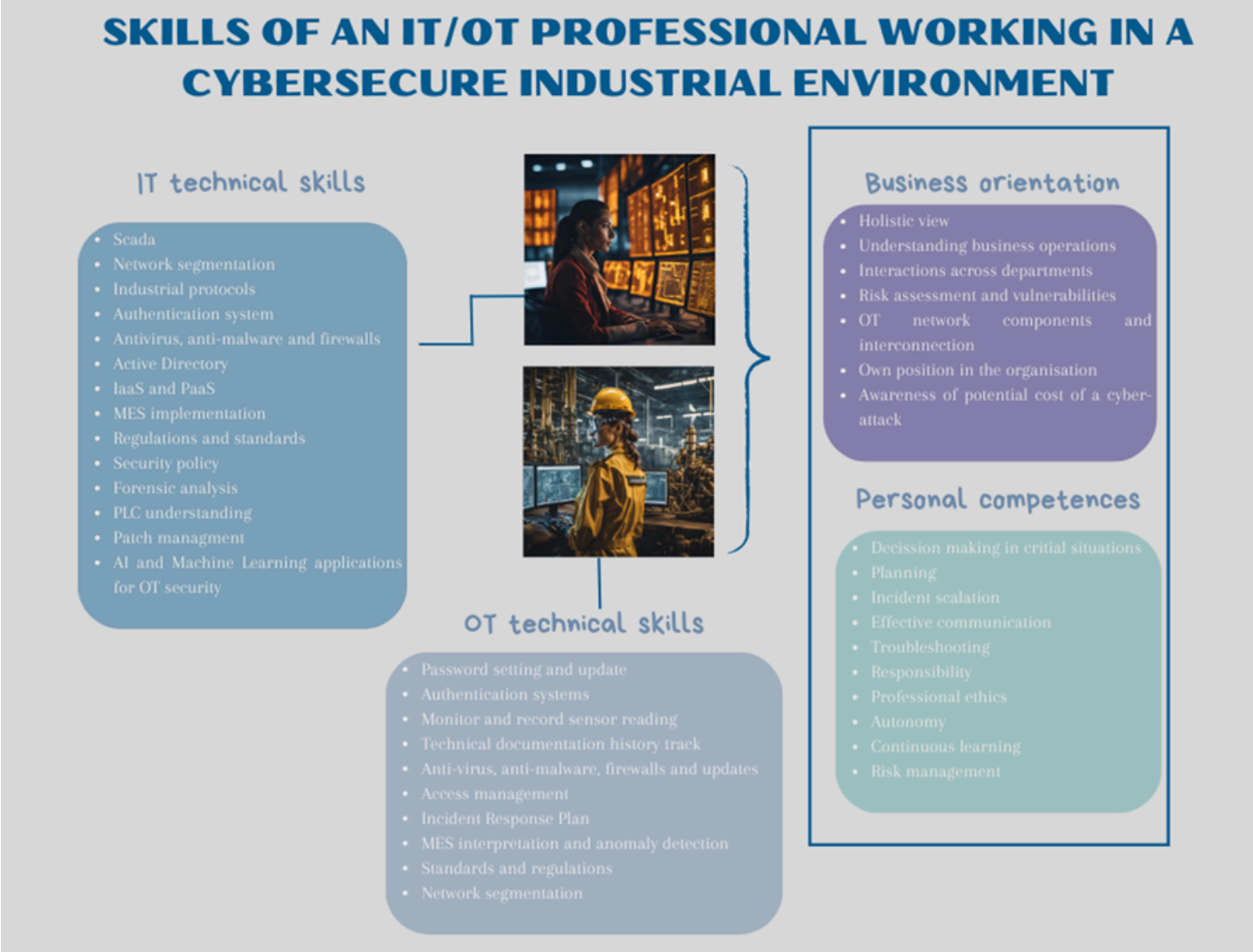
BUSINESS ORIENTATION

The capacity to understand the company globally as well as being able to position within the company´s scheme. It also includes the ability to assess the potential risks of a cyber attack to the company, as well as the impact it could have on human safety, production capacity or sensitive data.

PERSONAL COMPETENCES

Competences which are necessary to interact with peers and across company departments, reflect and think critically, solve problems, analyse situations from different perspectives, work autonomously but also being part of a team and act as a team player.

We have grouped the skills detected as gaps in each curriculum according to the mentioned classification. The technical skills are specific for the each profile (IT/OT), but the ones lying under the categories “business orientation” and “ personal competences”, in what regards cybersecurity, are the same for both.



Whereas in the different countries there are options to continue studying and specialising in industrial cybersecurity addressed to both OT and IT VET profiles, the approach of Cyber-In is to understand cybersecurity skills as transversal to any professional and, particularly, industrial cybersecurity transversal to IT and OT professionals, specially those further involved in industrial automated processes, as demanded by companies.

In order to provide safe industrial environments with a high level of automation (understanding safety from all possible points of view), cybersecurity needs to be embedded in the curriculum of IT and OT professionals.

Moreover, the demands from industry go towards a hybrid/interdisciplinary profile IT/OT, specialist in inudstrial cybersecurity. Whereas embedding learning outcomes related to cybersecurity in current IT and OT profiles delivered in the different countries will enhance the preparation of these professionals,, our recommendation as result of our findings is to offer an interdisciplinary VET curriculum in industrial cybersecurity as a specialization for both types of professionals.

We have defined such a curriculum aligned with EQF and ECVET frameworks, using a modular structure which can be splitted up into microcredentials to facilitate acquiring and accrediting the necessary competences.

An interdisciplinary VET curriculum in industrial cybersecurity

Curriculum structure and integration into existing VET programmes

This interdisciplinary curriculum integrates Information Technology (IT) and Operational Technology (OT) cybersecurity competences into a specialization programme addressed to graduates/workers from these fields. It addresses the skills gaps identified in the Cyber-In report on companies´ needs and promotes collaborative security practices in OT environments, ensuring that graduates/workers in this field are able to design, implement, and maintain secure industrial systems.

The curriculum aligns with ESCO profiles such as "cybersecurity technician" and "industrial automation technician" covering competences common to these 2 profiles. It has been structured using ECTS principles, where 1 credit is equivalent to approximately 25 learning hours.

The total amount of hours of the curriculum is approximately 250 hours , equivalent to 10 credits ECTS. According to the European Qualifications Framework and considering this specialization programme addresses primarily already graduates from IT/OT VET programmes with a EQF level 4-5, the specialization progamme has been conceived as a EQF level 5 itself.

While the development of the full interdisciplinary curriculum proposed by the Cyber-In project is encouraged, the aim of Cyber-In is not to develop a specialization programme to be completed as an addition to current IT and OT VET degrees but EMBED some of the learning outcomes (knowledge, skills and competences) defined in the curriculum and identified by the companies interviewed by the project partners as transversal and essential for a professional in IT network administration and management and operators in automated and interconnected industrial environments.

An interdisciplinary VET curriculum in industrial cybersecurity

Curriculum structure and integration into existing VET programmes

Therefore, we have designed a shorter course which addresses the mentioned learning outcomes and that can be more easily embedded in current programmes because:

- It has a shorter duration and is fragmented in short modules and chapters, facilitating its integration in current contents already taught in IT and OT VET programmes.

- Impacts particularly in attitude aspects and influences in the human factor and the conception of cybersecurity as part of the business culture.

- Targets key concepts, definitions and tools related to industrial cybersecurity. It doesn´t go in depth in the technical aspects but still covers the essentials and gives room to focus on particular aspects of industrial cybersecurity depending of the purpose of the course or the learnign objectives set by the teacher/trainer or worker in the case of employees or recent graduates.

The Cyber-In MOOC enable learners to understand the main concepts and elements related to industrial cybersecurity. It enables them to use and interpret monitoring tools, analyse potential risks and vulnerabilities and take a proactive approach to minimise breaching risks. It also provides learners with knowledge about the latest regulations related to cybersecurity in industrial environments and how those affect businesses and their roles as professionals.

The MOOC is open, no registration needed, to any user with an interest in improving those competences. The access is available through the project website: www.cyber-in.eu, under the section “learning resources”.

An interdisciplinary VET curriculum in industrial cybersecurity

Curriculum structure and integration into existing VET programmes

Module title	ECTS Credits	Duration
Module 1. Introduction to cybersecurity in OT environments	0.4	10 hours
Module 2. Segmentation and industrial protocols	1.6	40 hours
Module 3. Intrusion Detection Systems (IDS) for business continuity management	1.2	30 hours
Module 4. OT cybersecurity standards and regulations	0.8	20 hours
Module 5. Centralised security management systems and AI applications	1.2	30 hours
Module 6. Business Continuity Management and Service delivery	0.8	20 hours
Module 7. Project: Securing a Smart Factory	4	100 hours

An interdisciplinary VET curriculum in industrial cybersecurity

Module descriptions

Module 1 — Introduction to cybersecurity in OT environments

Duration: 10 hours | 0.4 ECTS credits

Objective: Understand cybersecurity fundamentals, IT–OT convergence, and industrial threat landscape.

Contents:

- Cybersecurity principles and definitions: CIA triad, defence in depth, risk vs. resilience.
- Differences between IT and OT priorities.
- Case studies: Stuxnet, BlackEnergy, Industroyer...

Learning outcomes:

- Knowledge: Explain OT principles, process control, and the CIA–Safety relationship.
- Skills: Identify OT system components and map them within a plant architecture.
- Competences: Recognize cyber–physical consequences of security breaches.

Assessment Methods: Group discussion, practical assessment, test.

Micro-credential 1: Cyber-In Module 1. Introduction to cybersecurityin OT environments

An interdisciplinary VET curriculum in industrial cybersecurity

Module descriptions

Module 2 — Segmentation and industrial protocols

Duration: 40 hours | 1.6 ECTS credits

Objective: Identify and classify industrial components and architectures using the Purdue Model.

Contents:

- OT components: PLCs, RTUs, SCADA, sensors, HMIs.
- System mapping, asset inventory and interdependencies.
- Industrial control hierarchy and data flow mapping.

Learning outcomes:

- Knowledge: Describe the Purdue model, network zones, conduits, and data flows.
- Skills: Apply segmentation and identify insecure protocols.
- Competences: Design and document an OT network segmentation plan.

Assessment Methods: Group discussion, practical assessment, test.

Micro-credential 2: **Cyber-In module 2. Segmentation and industrial protocols**

An interdisciplinary VET curriculum in industrial cybersecurity

Module descriptions

Module 3 — Industrial Networks & Protocol Security

Duration: 30 hours | 1.2 ECTS credits

Objective: Secure industrial protocols and communications channels.

Contents:

- Modbus, OPC-UA, PROFINET, DNP3, and MQTT security.
- Network analysis and packet inspection tools.
- Design and implementation of secure channels (TLS, VPNs).

Learning outcomes:

- Knowldege: Next- Generation firewalls
- Skills: Configure IDS/IPS sensors, interpret alerts, evaluate anomalies.
- Competences: Correlate monitoring data with operational safety needs and propose corrective actions.

Assessment Methods: Group discussion, practical assessment, test.

Micro-credential 3: **Cyber-In Module 3. Intrusion Detection Systems and Security in Firewalls**

An interdisciplinary VET curriculum in industrial cybersecurity

Module descriptions

Module 4 — OT cybersecurity standards and regulations

Duration: 20 hours | 0.2 ECTS credits

Objective: Learn the main standards and regulations in OT cybersecurity

Contents:

- EU cyber resilience Act
- IEC 62443
- Cybersecurity evaluation and types of tests

Learning outcomes:

- Knowledge: Difference between directive, standard and regulation
- Skills: Pentesting and vulnerabilities detection
- Competences: Accomplishment with standards and regulations

Assessment Methods: Group discussion, practical assessment, test.

Micro-credential 4. Cyber-In module 4. OT cybersecurity standards and regulations

An interdisciplinary VET curriculum in industrial cybersecurity

Module descriptions

Module 5 — Centralized security management systems and AI applications

Duration: 30 hours | 1,2 ECVET/ECTS credits

Objective: Apply relevant standards and conduct industrial cybersecurity risk assessments.

Contents:

- Centralized Security Management
- AI applications
- Governance and policies

Learning outcomes:

- Knowledge: Understanding of CMS
- Skills: identify essential roles, policies and procedures for security governance
- Competences: Apply CMS and use AI applications for threat detection and response

Assessment Methods: Group discussion, practical assessment, test.

Micro-credential 5. Cyber-In module Centralized Security Management Systems And Real-Time Threat Detection In Enterprise It Environments

An interdisciplinary VET curriculum in industrial cybersecurity

Module descriptions

Module 6 — Business Continuity Management and Service delivery

Duration: 20 hours | 0,8 ECTS credits

Objective: Integrate safety engineering and cybersecurity in critical infrastructures.

Contents:

- Business continuity managent concept and challenges
- Best practices
- Service Delivery
- ITIL

Learning outcomes:

- Knowledge: Understand BCM, Service Delivery and Zero Trust concept
- Skills: How to ensure continuity management and service delivery
- Competences: Apply recovery strategies and design Incident Response Plans

Assessment Methods: Group discussion, practical assessment, test.

Micro-credential 6 — Cyber-In module Business Continuity Management and Service Delivery

An interdisciplinary VET curriculum in industrial cybersecurity

Module descriptions

Module 7 — Project. Securing a smart factory

Duration: 100 hours | 4 ECTS credits

Objective: Apply all competences acquired in previous modules in a simulated smart factory scenario.

Contents:

- Team-based design and implementation of a secure industrial network.
- Security testing, risk mitigation, and incident management.
- Project presentation.

Learning outcomes:

- Knowledge: Integrate OT design, risk management, and standards and regulation concepts.
- Skills: Develop and present an industrial cybersecurity plan.
- Competences: Justify design and security decisions made.

Assessment Methods: Group discussion, practical assessment, test.

Micro-credential 7. Challenge based learning activity

Conclusions

OT cybersecurity increases customer trust and ensures operational continuity

Companies in the involved countries recognize that cybersecurity offers numerous advantages, including increased customer trust, protection of sensitive information, and ensuring operational continuity. The benefits of securing the OT environment clashs against the challenge of finding IT professionals with specific knowledge of OT networks as well as OT professionals with the adequate level of awareness of cybersecurity risks and enough autonomy and technical skills to play a role in the overall cybersecurity architecture of the company.

Increasing awareness and training is, therefore, crucial to improve cybersecurity in industrial environments with a high level of automation. Companies that prioritize continuous training, collaboration between IT and OT departments, and the implementation of best practices are better equipped to protect their critical infrastructures and maintain operational continuity.

Sensitization and training in technical and personal skills is crucial

A combination of personal competences, technical skills and a holistic approach to the company is highly demanded, including the capacity for collaboration between IT and OT departments to ensure an effective security approach.

The reality, however, in vocational schools at the moment is that the IT and OT curricula are not responding to these demands. There is a general lack of attention to cybersecurity in IT VET programmes when referring to industrial environments, and this lack of attention to cybersecurity is absolute in OT programmes. We could state that the main problem for IT professionals is the lack of knowledge and skills about an OT network whereas the deficiency in OT professionals starts in the lack of awareness. This reality is common to all partner countries, thus, the gaps detected in both types of professionals regarding cybersecurity skills are almost the same.

Taking this reality as a basis, there is no other option than start building awareness and knowledge by integrating cybersecurity in IT and OT curricula as a transversal skill, starting with teachers and trainers and cascading down to students.

Aknowledgements

We want to thank the companies involved in the Cyber-In project, in particular those participating in the national focus groups for their availability, enthusiasm and commitment to improve continuous vocational education. Their contribution has been essential not only to develop this report and to implement future project steps but also to update the knowledge, skills and competences of all project staff, teachers and students involved.

A special recognition goes to the 5 entitites which have reviewed, assessed and validated the modular curriculum proposed by Cyber-In. A big THANK YOU goes to Secure Network SRL (IT), Cybasque (ES), Rapla County Vocational College (Estonia), NTO Automation (DK) and OIXIO (Estonia).

Contact Us

Phone

+ 31 088-6572657

Email

rbezemer@davinci.nl

Website

www.cyber-in.eu

Address

Leerparkpromenade 100
3312 KW Dordrecht
Netherlands