Industrial CyberSecurity 4.0 : Preparing the Operational Technicians for Industry 4.0

Konstantinos Karampidis[1], Giorgos Papadourakis[1], Spyros Panagiotakis[1], Manos Vasilakis[1], Maria Christofaki[1], Nuno Escudeiro[2], Anabel Menica[3], Jokin Goioaga[3], Aris Chronopoulos[4]

[1]Hellenic Mediterranean University, Heraklion, Crete, Greece
[2]Instituto Superior de Engenharia do Porto, Porto, Portugal
[3]Politeknika Ikastegia Txorierri, Spain
[4]IDEC S.A., Piraeus, Greeece

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

About InCys4.0

- **InCyS 4.0 (Industrial CyberSecurity 4.0)** is a 2-year project co-funded by the Erasmus+ programme of the European Union, started in October 2018 and it involves 4 partners across Europe.
- Industry needs trained technicians and engineers capable to identify potential cybersecurity threats and able to respond adequately when an attack is identified
- Personnel training in these skills is costly

About InCys4.0

- The programme aims to offer open source course materials and Higher Education (HE) training to fill the evident gap in awareness and competence in cyber security for operational technicians in Industry 4.0.

InCyS 4.0 Partners

- **Coordinator**: Politeknika Ikastegia Txopierri, Spain
- **Partner**: Insituto Superior de Engenharia do Porto, Portugal
- **Partner**: Hellenic Mediterranean University, Crete, Greece
- **Partner**: IDEC SA , Piraeus, Greece

Overall Impact

InCyS 4.0 project will improve the professional competence of the students, teachers, professors and employers in the industrial automation field by training them in cyber security awareness and responsiveness.

Overall Impact

On Students:

- Industrial students from EQF level 5 and above will be trained in awareness and responsiveness to cyber security risks related to modern ICS
- They will be more competitive when looking for a job as enterprises need operational technicians capable of managing and responding to the new realities of integrated connectivity in Industrial production and processes.

On Project Partners:

- All the partner centers will use InCyS 4.0 outputs in technical courses involving automation, robotics, programming production, mechatronics, I.T and Systems, updating education in line with the needs of Industry 4.0. This offers Politeknika Txorierri, IPP, HMU and IDEC a plus in innovation and attractiveness; educational responsiveness to Industry and the satisfaction of preparing students to the highest possible standard.
- The InCyS 4.0 project fosters cooperation between high level VET/ HE institutions and industrial enterprises thus strengthening the “knowledge triangle” linking education, research and Industry.
-

Overall Impact

On Professors/Teachers/ Trainers:

- Their educational work is facilitated by the implementation of ready to use innovative project outputs - industrial cyber security for OT
- Opportunities for professional development; piloting the InCyS 4.0 Training Course engages teachers in innovation and they gain in motivation and confidence regarding their professional skills
- Teachers have access to free open source educational materials which are easily adaptable for different training channels and courses. They can offer related services to clients and collaborators via their networks and training provision for the unemployed or employed technicians who require upskilling
- Participating staff also benefit from transnational exchange and knowledge transfer = knowledge growth

Overall Impact

On Industrial Enterprises:

- Enterprises (especially SMEs) save money in training operational technicians
- Industrial companies in process of modernising gain in security and responsiveness to cyber risks
- The industrial sector is strengthened adding greatly to competitiveness and prosperity. In the Basque Country (ES), automated Industry is one of the 5 key RiS3 strategies for prosperity.

On Higher Vet Centers/ He Institutions/

- Higher VET/ HE Institutions are invited to integrate a Course for training students in operational cyber security for Industry 4.0 that is practical, adaptable and which meets industry demands
- Constant modernization of their organizations and educational offer.

Research

- The partnership carried out a research among enterprises or SMEs.
- Field research had the form of an anonymous questionnaire targeting the IT personnel of local industries, so the project investigates the security weaknesses of the participating enterprises and adapt its training content according to the feedback.
- From each partner country, at least 10 representative large enterprises or SMEs participated.

Research outcomes

- **Do you implement a security policy at your enterprise?**
  - 80% of the enterprises answered they implement a security policy at their organization.
- **What is your password policy?**
  - 55% of the enterprises answered that they don't have a password policy. From the rest 45% that implements a password policy, only ¼ of them has very strict rules.
- **Do you implement any monitoring and control measures of those who have access to each part of the automation production process?**
  - Although most of the companies have monitoring and control measures of those who have physical access to each part of the automation production process, only 42% of them keep detailed log files.

Research findings

- **Is your network equipment physically secured in a restricted access room?** Only 60% of the companies have their network equipment physically secured in a restricted access room.
- **Do you implement any update/upgrade policy for the firmware used in your automation mechanisms?** 65% of the enterprises answered that they don’t have an update/upgrade policy.
- **Are your workers allowed to connect their own devices to the enterprise network?**

  Employees are usually allowed (70%) to bring their own devices at work, although the use of their personal computers is prohibited.

Research findings

- **Do you implement any scheduled awareness briefing for the operators on security themes like phishing, social engineering attacks, tailgating, etc.?**
  70% of the enterprises don’t have scheduled awareness briefing for their operators on security themes.
- **Can you estimate the cost of recovering the current status of your automation network in case of a major disruption caused by a security breach?**
  67% of the enterprises cannot estimate the cost of recovering their automation network from a major disruption caused by a security breach.
- **Do you implement a firmware and configuration backup strategy for your automation devices?**
  60% of the enterprises implement a firmware and configuration backup strategy for their automation strategies. From these enterprises only 50% check their backups regularly.

Research findings

- **Is your network segmented into separated subnetworks for IT (office network: PC's and servers) and OT (automation network: PLC, HMI, sensors/actuators)?**
  Only 30% of the participating enterprises have their networks segmented into different subnetworks for IT and OT.
- **Do you have configured a firewall to control the traffic between IT and OT networks?**
  The majority of the enterprises (83%) have configured a firewall to control the traffic between the two networks.
- **Does your organization use manageable switches in order to control and monitor network traffic?**
  60 % of the companies do not use manageable switches

Research findings

- **Does your organization have deployed any traffic analysis tool to detect abnormal traffic or unauthorized connections?**
  75% of the organizations do not have deployed any such traffic analysis tool.
- **Does your organization have any antivirus solution deployed in order to detect infected hosts?**
  Only 50% of the organizations have deployed anti-virus solutions for the detection of infected hosts.
- **Is it possible to remotely access (remote Desktop, remote sessions) your organizational OT network?**
  70% of the enterprises allow remote access to their organizational OT network

Research findings

- **Is remote access controlled by a firewall?**
  65% of the enterprises which allow remote access, have it controlled by a firewall.
- **Do you have any contingency plan in case of a cyber-attack?**
  50% of the enterprises do not have a contingency plan.
- **Does your organization use secure connections towards your network equipment (VPN, SSH tunnels)?**
  The majority of the companies (70%) allow secure remote connections to their systems, but there is a critical 30% that do not.

Research findings

- **Does your organization allow WLAN connections on the OT network?**
  70% of the organizations allow WLAN connections on their OT network.
- **Does the OT WLAN connection use WPA2?**
  All of the enterprises that allow WLAN connections on their OT networks have them secured with WPA2 protocol.
- **Does your OT WLAN setup authenticate the clients (RADIUS server or certificates)?**
  Only 43% of the OT WLAN setups authenticates the clients.
- **Does your OT WLAN setup filter clients using MAC addresses?**
  65% of the OT WLAN setups do not filter clients using MAC addresses.

Training Modules

Following the outcomes of this research, partners worked on the structure of the Course and the structure of the description of the modules and learning outcomes. Below is the final structure of the course separated into 3 Modules:

- **Module 1 - Industrial Systems: Components And Characteristics**
- **Module 2 - Security Concepts In Industrial Environments. Integration Of IT/OT**
- **Module 3 - Confidentiality, Integrity, Availability In Industrial Environments**

Each module is separated into several units which are presented in the next slides

Module 1 - Industrial Systems: Components And Characteristics

- **Components**
  - Business information console
  - Supervisory workstations
  - HMI interfaces
  - Controllers: PLC, RTU, IED
  - Sensors: types and characteristics
  - Actuators: types and characteristics

Module 1 - Industrial Systems: Components And Characteristics

- **System architecture**
  - Control loops
  - Feedback loops
  - Business management
  - Production management
  - Process management
  - Safety instrumented systems

Module 1 - Industrial Systems: Components And Characteristics

- **Network design and architecture**
  - DCS, SCADA
  - ISO levels
  - Topologies: mesh, ring, star, bus, wireless mesh
  - Connectivity: serial (RS232/485) , IP/Ethernet
  - Segmentation: switch, router, firewall. Physical/logical (VLAN….)
  - Redundancy
  - Remote access (Telnet , SSH, Remote Desktop , Teamviewer, VNC)
  - Performance: latency, bandwidth, QOS, network hops, Real Time isochronus Networks
  - Wide area, Smart Grid, Metering

Module 1 - Industrial Systems: Components And Characteristics

- **Industrial Network Protocols**
  - Real time protocols
  - Fieldbus protocols:
    - Modbus
    - Profibus
    - Profinet
  - Industrial Ethernet
  - Backend protocols:
    - OPC

Module 2 - Security Concepts In Industrial Environments. Integration Of IT/OT

- **Security in critical infrastructures / installations**
  - Plant security
  - Network security
  - System integrity
- **OT/IT integration**
  - Definition
  - Advantages - Disadvantages
  - Policies regarding the updates for computers and PLCs

Module 2 - Security Concepts In Industrial Environments. Integration Of IT/OT

- **Attacks on industrial systems**
  - Denial-of-Service (DoS) Attack
  - Man-in-the-Middle (MitM) Attacks
  - Modbus/TCP Protocol Attack
  - Dictionary Attack
- **Information Society Law of Services and Electronic Commerce**
  - Definition

Module 3 - Confidentiality, Integrity, Availability In Industrial Environments

- **Data confidentiality**
  - Data storage
  - Data transport
- **Data integrity**
  - Data storage
  - Data transport
- **Availability**
  - Error tolerance
  - Contingency plan
  - System recovery

Module 3 - Confidentiality, Integrity, Availability In Industrial Environments

- Modular content will be created using eXelearning software (a free software tool under GPL-2 that can be used for creating interactive educational web content).
- All the educational materials will be integrated into a LMS (Learning Management System) like Moodle. As such, the InCyS 4.0 Course content will be highly transferable in terms of access for integration into existing industrial educational programmes or other training options.
- The produced open source content, along with relevant activities in the three modules and the quick guide, will be sporadically available online on the project's website : http://www.incybersecurity.eu/

Thank you!

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