



A hands-on Approach to Cybersecurity Training for Industrial Technicians

**Konstantinos Karampidis, Spyros Panagiotakis, Manos Vasilakis, Evangelos K. Markakis, Maria Christofaki,
Giorgos Papadourakis**
Hellenic Mediterranean University
Heraklion, Greece

Nuno Escudeiro, Felipe Santos
Polytechnic Institute of Porto
Porto, Portugal

Anabel Menica, Jokin Goioaga
Politeknika Ikastegia Txorierrri
Derio, Bizkaia, Spain

Aris Chronopoulos, Antonio Gennarelli
IDEC SA
Piraeus, Greece

Martina Manfredda
DLEARN
Milan, Italy



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

About DICYTECH

- With the emergence of industry 4.0, the plants of existing industries are transformed into smart ecosystems equipped with various solutions based onto Internet networking.
- Cyberphysical attacks grow dramatically recently.
- Industrial IT operators do not consider this likelihood seriously.
- In the new ecosystem, an intrusion by cyber-attackers into the virtual. cyberspace of an enterprise is a far more obvious issue than any physical attack against the physical establishments of a plant.

About DICYTECH

- **DICYTECH** (Digital Training for Cybersecurity Students in Industrial Field) is a 2-year project co-funded by the Erasmus+ programme of the European Union, started in April 2021 and it involves 5 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 DICYTECH



- The programme aims to offer:
 - open-source course materials and Higher Education (HE) training (IO1) to fill the evident gap in awareness and competence in cyber security for operational technicians in Industry 4.0.
 - three (3) developed and tested cybersecurity labs (IO2) in 3 partner HE organisations (Txorierrri/IPP/HMU) accessible remotely through an online DICYTECH HUB for distance learners.

DICYSTECH 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
- **Partner:** European Digital Learning Network DLEARN , Milan, Italy

Overall Impact

On Students:

- Industrial students from EQF level 5 and above are trained in awareness and responsiveness to cyber security risks related to modern ICS.
- They are 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 use DICYTECH 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, IDEC and DLEARN a plus in innovation and attractiveness; educational responsiveness to Industry and the satisfaction of preparing students to the highest possible standard.
- The DICYTECH 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 Industrial Enterprises:

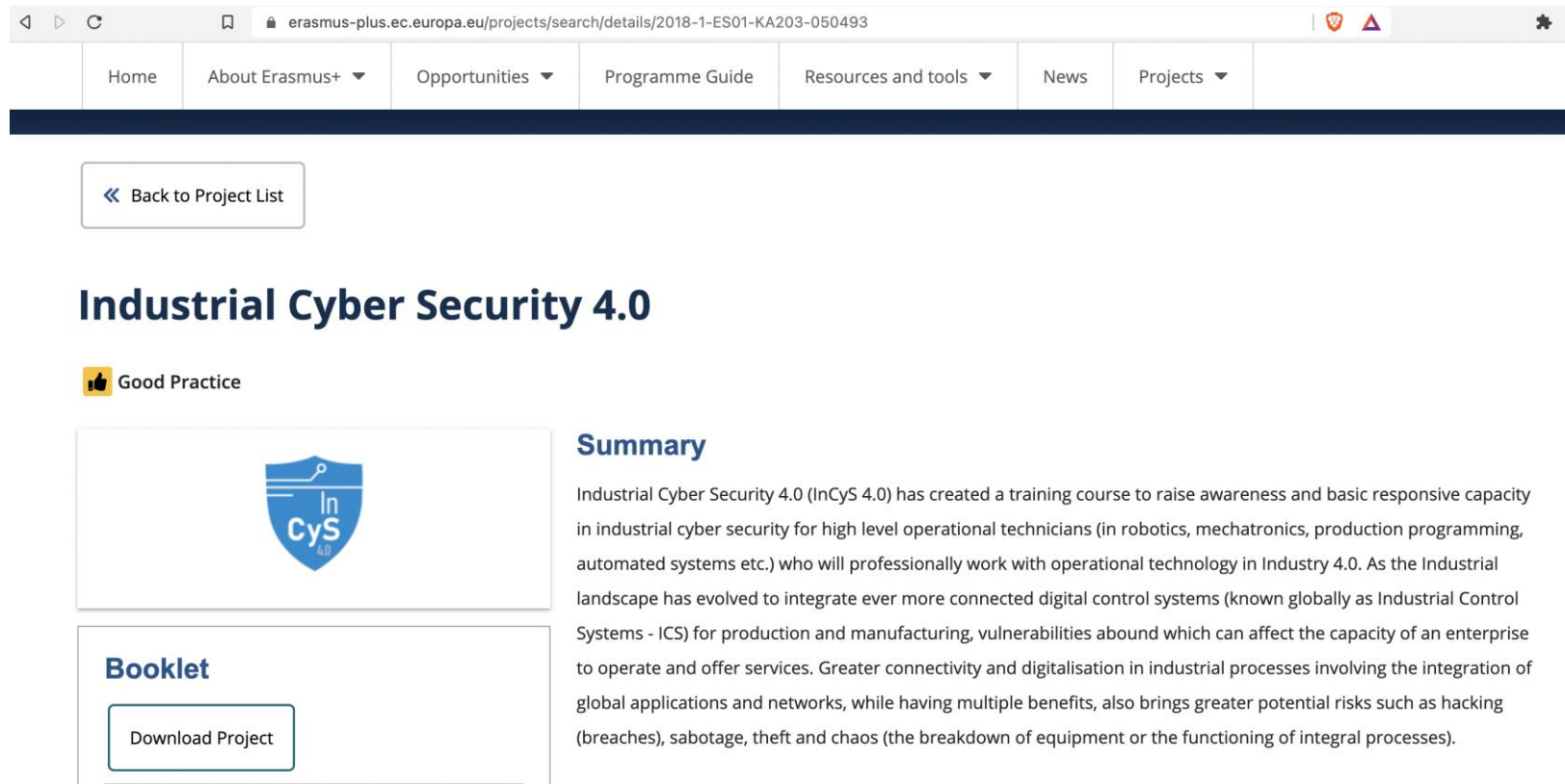
- Enterprises (especially SMEs) save money in training operational technicians.
- Industrial companies in process of modernizing gain in security and responsiveness to cyber risks.
- The industrial sector is strengthened adding greatly to competitiveness and prosperity. In the Basque Country (ES), automated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

Background

DICYTECH is the continuation of the EU funded project [InCyS 4.0](#). EU has characterized InCyS 4.0 as a good practice example.




The screenshot shows a web browser window with the URL erasmus-plus.ec.europa.eu/projects/search/details/2018-1-ES01-KA203-050493. The navigation menu includes Home, About Erasmus+, Opportunities, Programme Guide, Resources and tools, News, and Projects. A button labeled "Back to Project List" is visible. The main content area features the title "Industrial Cyber Security 4.0" with a "Good Practice" badge. Below the title is a logo for InCyS 4.0. A "Booklet" section contains a "Download Project" button. A "Summary" section provides a detailed description of the project's goals and impact.

Home About Erasmus+ Opportunities Programme Guide Resources and tools News Projects

« Back to Project List

Industrial Cyber Security 4.0

👍 Good Practice



Summary

Industrial Cyber Security 4.0 (InCyS 4.0) has created a training course to raise awareness and basic responsive capacity in industrial cyber security for high level operational technicians (in robotics, mechatronics, production programming, automated systems etc.) who will professionally work with operational technology in Industry 4.0. As the Industrial landscape has evolved to integrate ever more connected digital control systems (known globally as Industrial Control Systems - ICS) for production and manufacturing, vulnerabilities abound which can affect the capacity of an enterprise to operate and offer services. Greater connectivity and digitalisation in industrial processes involving the integration of global applications and networks, while having multiple benefits, also brings greater potential risks such as hacking (breaches), sabotage, theft and chaos (the breakdown of equipment or the functioning of integral processes).

Booklet

Download Project

Background

- In InCyS 4.0, the partnership carried out a statistical research among enterprises or SMEs.
- Field research had the form of an anonymous questionnaire targeting the IT personnel of local industries, so the project investigated the security weaknesses of the participating enterprises and adapted its training content according to the feedback.
- From each partner country, at least 10 representative large enterprises or SMEs have participated.

Outcomes

Based on the findings of InCyS 4.0 the partnership has developed a **more advanced course** -comprised of five (5) modules-, and **three fully developed remote cybersecurity laboratories** in which learners can practice, experiment and develop their cybersecurity skills in a simulated industrial context.

The Course

Partners worked on the structure of the Course and the learning outcomes. The course (IO1) will include 5 Modules - 4 technical modules and 1 transversal module on soft skills- covering:

- **Module 1** - Industrial Networks (protocols and equipment)
- **Module 2** - Equipment Protection
- **Module 3** - Industrial Control Systems (ICSs) Protection: penetration testing, secure system design, incident response and tool development
- **Module 4** - Forensic Analysis of Industrial Networks: Countermeasures
- **Module 5** - Soft Skills for Cybersecurity: Communication, Teamwork and Problem Solving

The Remote Labs

Three (3) cybersecurity labs were developed and tested (IO2) in 3 partner HE organisations (Txorierrri/IPP/HMU) accessible remotely through an online DICYTECH HUB for distance learners.

The participant can reserve the lab he prefers through the use of the DICYTECH HUB and remotely practice in real world cybersecurity scenarios.

The Remote Labs - Scenarios

Scenario 1 - SQL Injection (HMU)

Scenario 2 - Modbus / PortScanning (Txorierri)

Scenario 3 - Modbus-based ICS Attack (Txorierri)

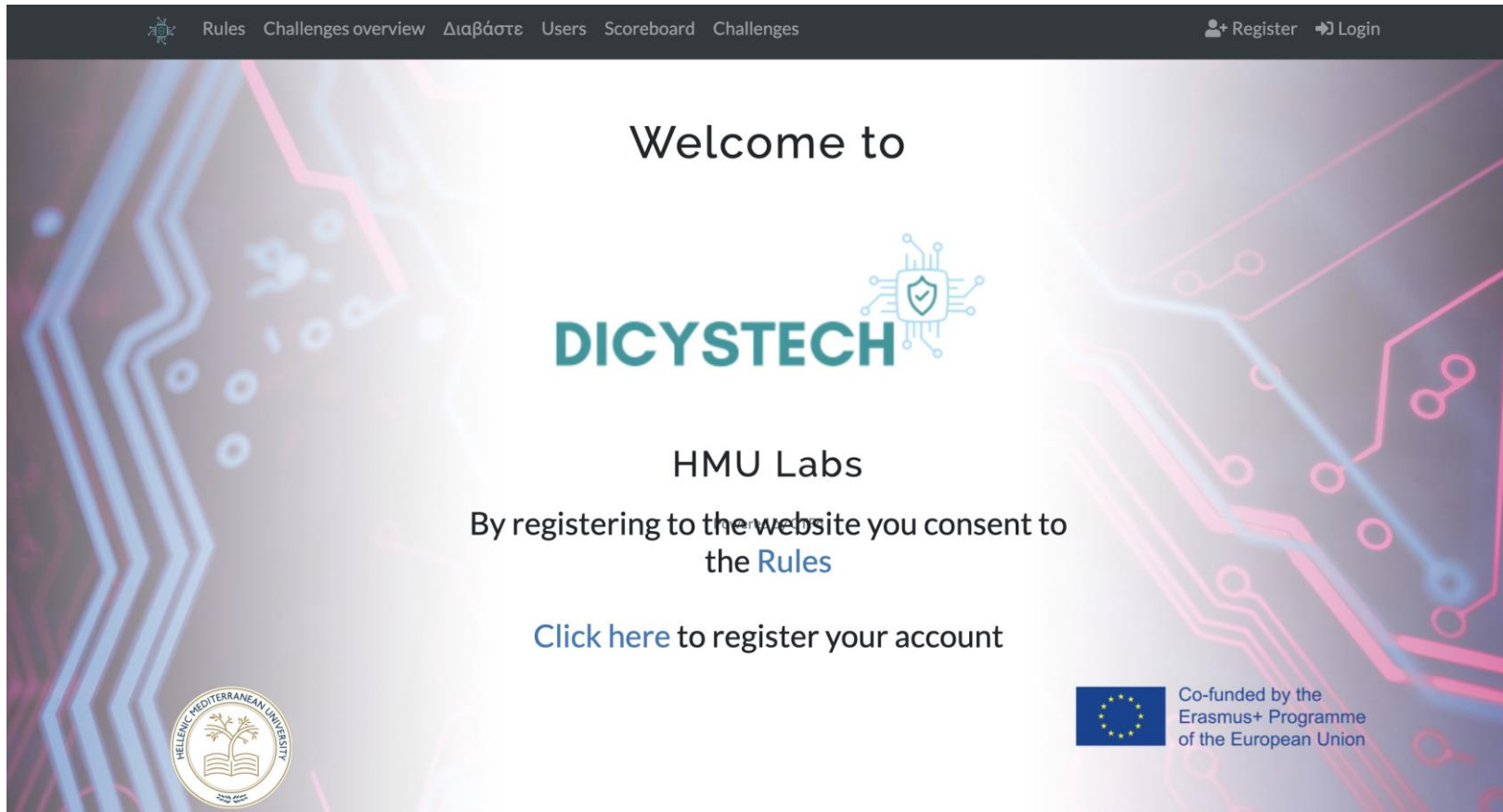
Scenario 4 – Man in the Middle (IPP)

Scenario 5 – Dos Attack -Snort Rules (HMU)

Scenario 6 – Forensic / Logs (HMU)

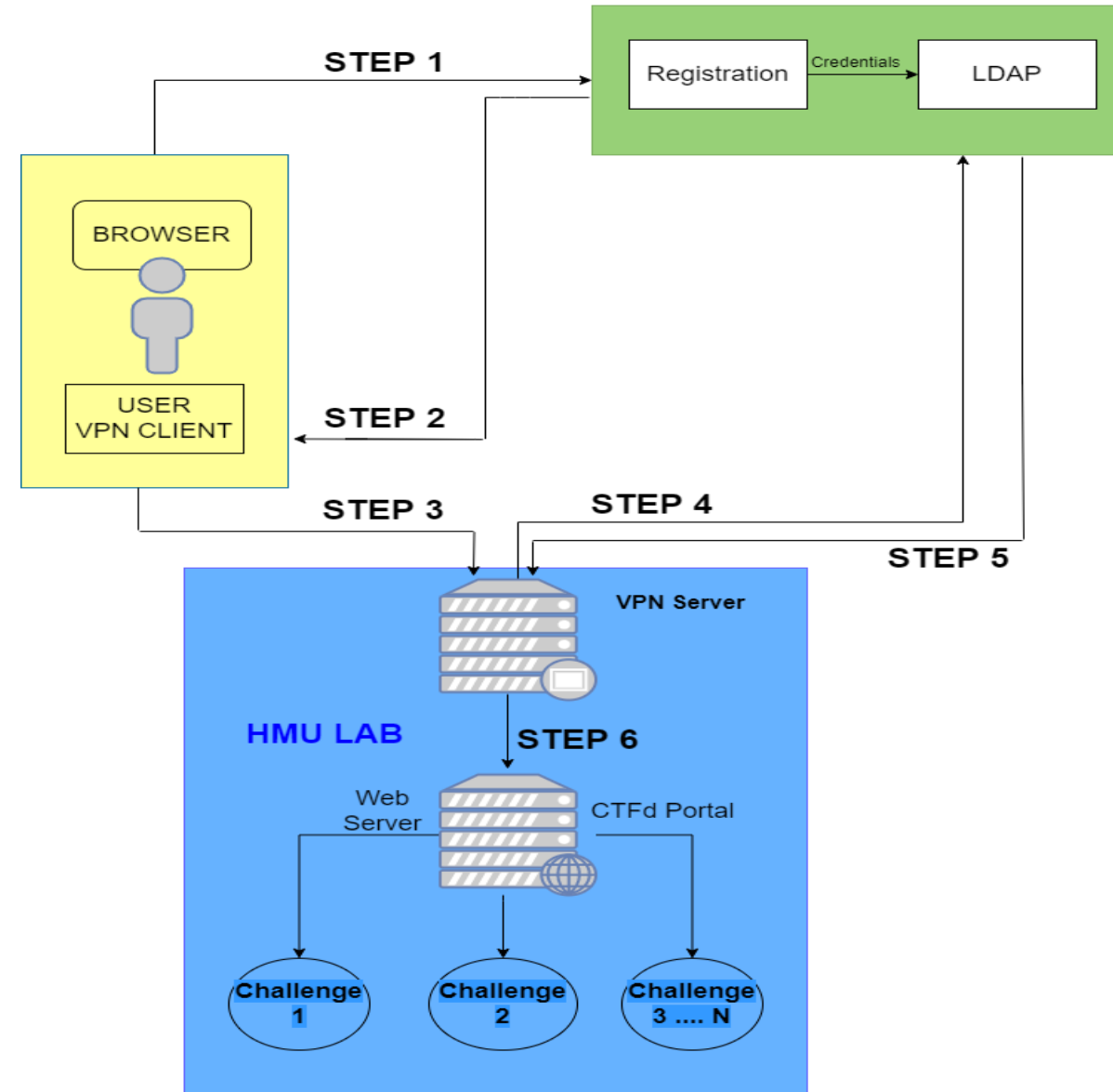
The Remote Labs – Implementation

All remote labs were implemented with [CTFd](#), an open-source Capture The Flag framework focusing on ease of use and customizability.

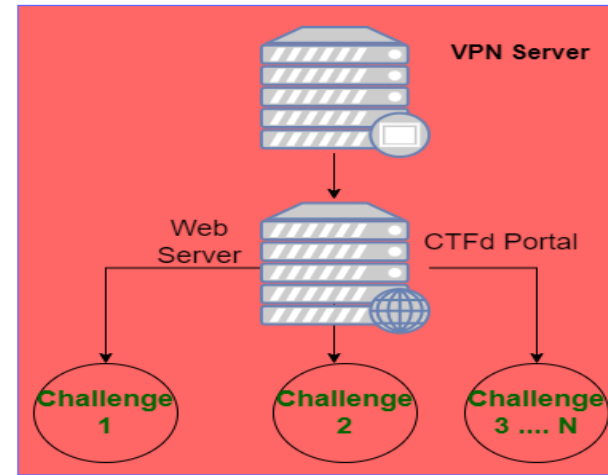


Remote Labs Architecture

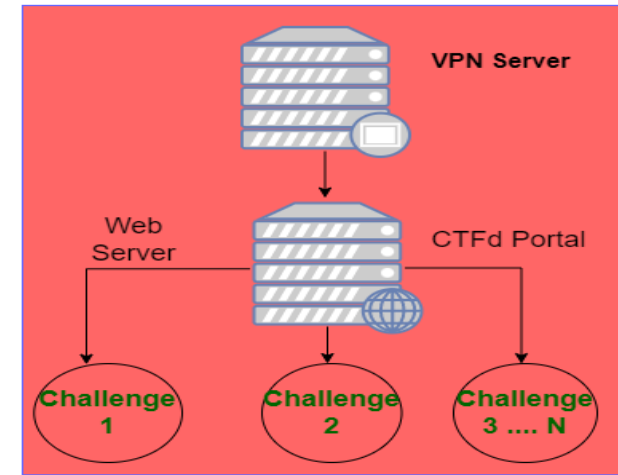
HUB



TXORIERRI LAB



IPP LAB



Training Material

- All the educational materials will be integrated into Moodle LMS (Learning Management System). This way, the DICYTECH Course content will be highly transferable in terms of access for integration into existing industrial educational programmes or other training options.
- All information regarding the project are available online on the project's website <https://dicystech.eu/>



Future Work

- **Pilot installations**
- **Multiplier Events**



Thank you!



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