EXAM 4.0

THE EXCELLENT ADVANCED MANUFACTURING 4.0

AM 4.0 labs running I4.0 technologies

Technology 5: Cybersecurity

5/15

Piloting the Advanced Manufacturing workshop 4.0

03

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

EXAM 4.0 partners:

TKNIKA – Basque VET Applied Research Centre, CIFP Miguel Altuna, DHBW Heilbronn – Duale Hochschule Baden-Württemberg, Curt Nicolin High School, Da Vinci College, AFM – Spanish Association of Machine Tool Industries, 10XL, and EARLALL – European Association of Regional & Local Authorities for Lifelong Learning.

TABLE OF CONTENTS

0. Introduction 05

1. Definition and application of cybersecurity in industry 06

2. Cybersecurity in HVET/VET labs 07

- 2.1. Cybersecurity in Tknika's Lab 07
- 2.2. Role of the cybersecurity in the EXAM4.0 CLF 10
- 2.3. Benefits of using cybersecurity in EXAM4.0's CLF 11
- 2.4. Competences addressed with cybersecurity 11

3. Collaboration opportunities opened by cybersecurity 13

4. References 14

This project has been funded with support from the European Commission. This publication 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 figures

Figure 1 Overall structure of the EXAM4.0 labs piloting process. Source: EXAM4.0

Figure 2 Tknika's cybersecurity lab's overview. Source: Tknika

Figure 3 Realtime honeypot attacks example. Source: Tknika

Figure 4 Omrom PLC area. Source: Tknika

Figure 5 Siemens PLC cell. Source: Tknika

Figure 6 EXAM4.0 Collaborative Learning Factory's (CLF) Value Chain Source:Author's creation

Introduction

Following the piloting process of Advanced Manufacturing Labs for H/VET through the Collaborative Learning Factory (hereafter CLF), the EXAM4.0 partners we have piloted 16 technologies embedded in Industry 4.0

The following image shows the overall structure of the piloting process.

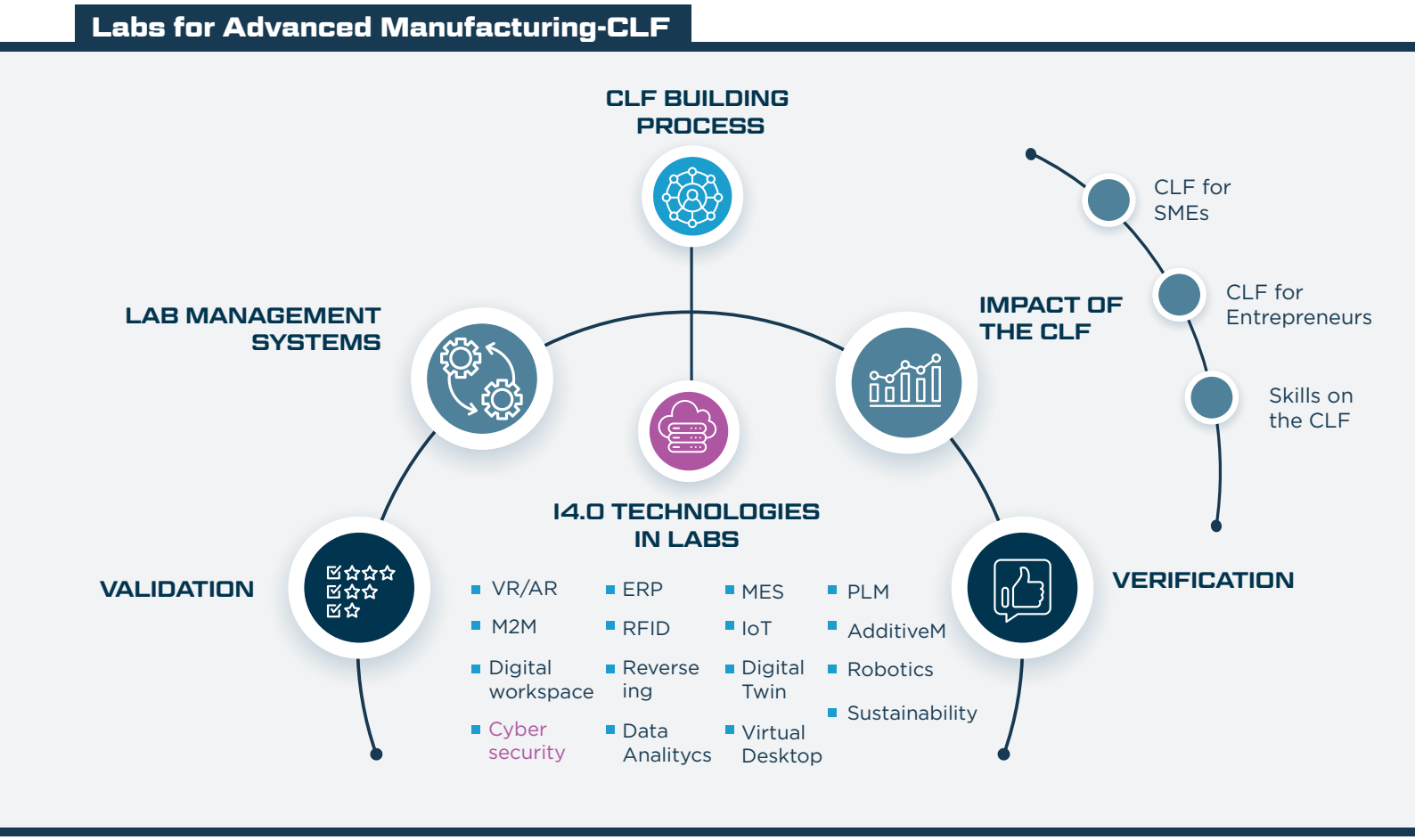

Figure 1: Overall structure of the EXAM4.0 labs piloting process.
Source: EXAM4.0

The present report is the one out of 16 I4.0 technology described within the "Industry 4.0 technologies in labs" section, specifically #5 Cybersecurity.

1 Definition and application of cybersecurity in industry

Cybersecurity is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. For a long time, this concept applied mostly to traditional IT devices, but with the spreading of the new 4.0 Industry, these practices had to be applied to any connected device. Cybersecurity is a trend in our more and more digitized and interconnected world. In order to respond to this need we simulate an industrial factory with IT and OT elements in our lab to provide different network casuistry, and create different scenarios where we can test protection and attack methods against our isolated networks, minimizing risks (Wikipedia, 2021).

2 Cybersecurity in HVET/VET labs

2.1. Cybersecurity in Tknika's Lab

In this section we address how Cybersecurity practices should be incorporated into the laboratories of VET / HVET centers with the aim at a safe performance of CLF processes. With this goal, we have been working in TKNIKA's Cybersecurity Factory Lab using different scenarios.

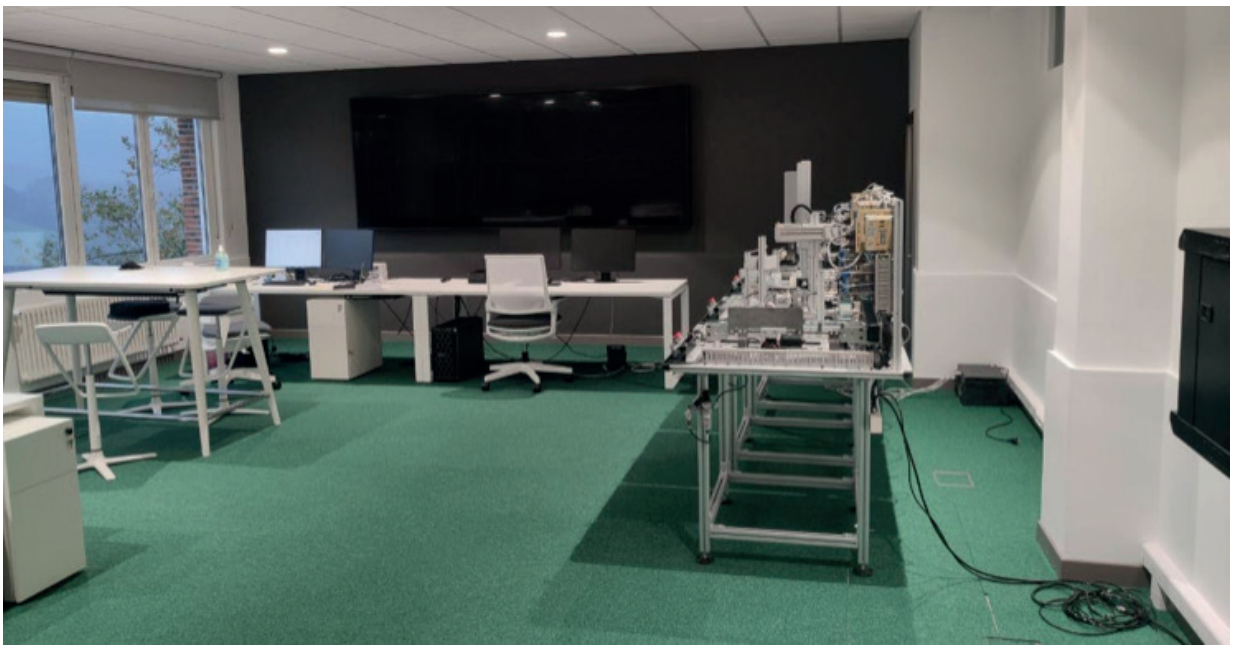

Figure 2: Tknika's cybersecurity lab's overview. Source: Tknika

Cybersecurity can be applied directly into two types of HVET/VET branches:

- On the one hand, we have IT related scenarios, which consist of an IT zone and a honeypot, as described in the WP4, section D4.2. In the IT zone, we have a rack with firewalls, switches and 3 PCs used to research the vulnerability of IT systems, in order to train in the creation and development of secure IT systems.

  In the honeypot zone we research what types of attacks an exposed device can get, where they come from, and how to mitigate them.

Figure 3: Realtime honeypot attacks example. Source: Tknika

The industry partners, as well as the students that make use of the Sustainability Factory, can use the datasets for development of prognostic algorithms and exploratory analysis.

Besides those specific branches, the basics and good usage of the Internet can be taught in any HVET/VET cycle to avoid information loss, ransomware, virus, malware…

In order to achieve all of this, different software is used, such as:

- Proxmox Virtual environment
- VMWare
- VirtualBox
- Modern Honey Network
- Visual Studio 2019
- PaloAlto Academy
- Wireshark
- Kali

Additionally, we have the industry and automation related escenarios, also described in the WP4, section D4.2., the Omrom PLC area and the Siemens PLCs area.

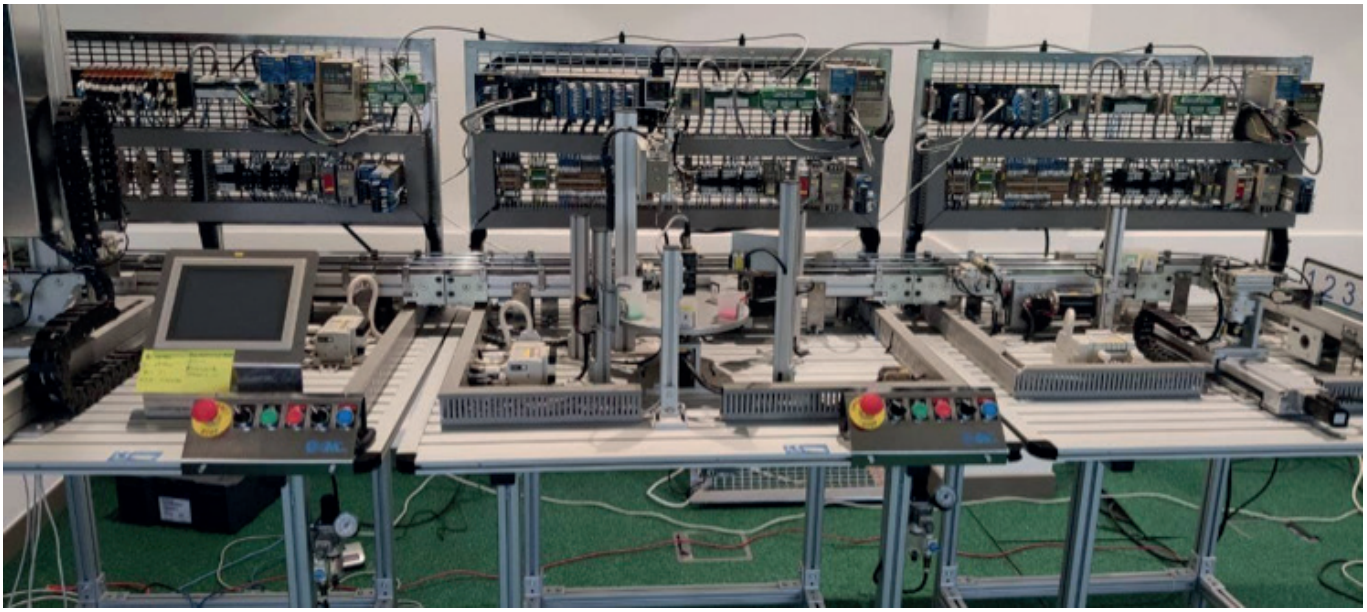

Figure 4: Omrom PLC area. Source: Tknika

Usually automation elements were isolated, but Industry 4.0 and remote assistance, among other factors, has forced these systems to be connected to the network. Due to lack of updating the automated systems, industry and automation related students should/must be aware of the danger and take action to protect them.

Overall, all IT systems must be protected. Not only the ones that are located in offices or server rooms but also in industrial machine HMI or Scadas.

In order to achieve all this, different software is used, such as:

- TIA Portal
- Cx One

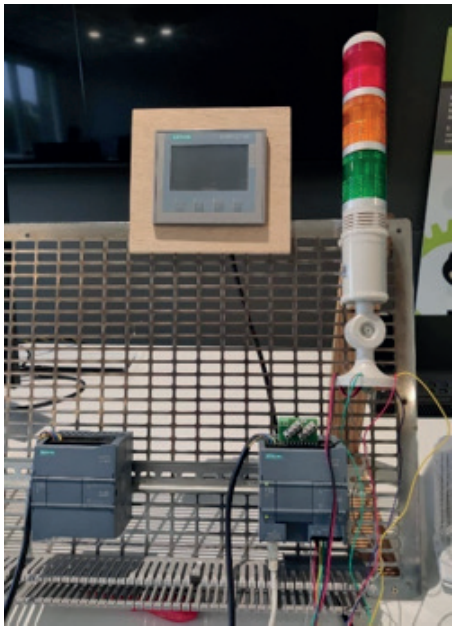

Figure 5: Siemens PLC cell. Source: Tknika

2.2. Role of the cibersecurity in the EXAM4.0 CLF

The CLF that is going to be launched has divided its production process into 4 stages (product design, process engineering, production and assembly) as can be seen in the following image. Within these stages, cybersecurity is going to be incorporated in the production stage.

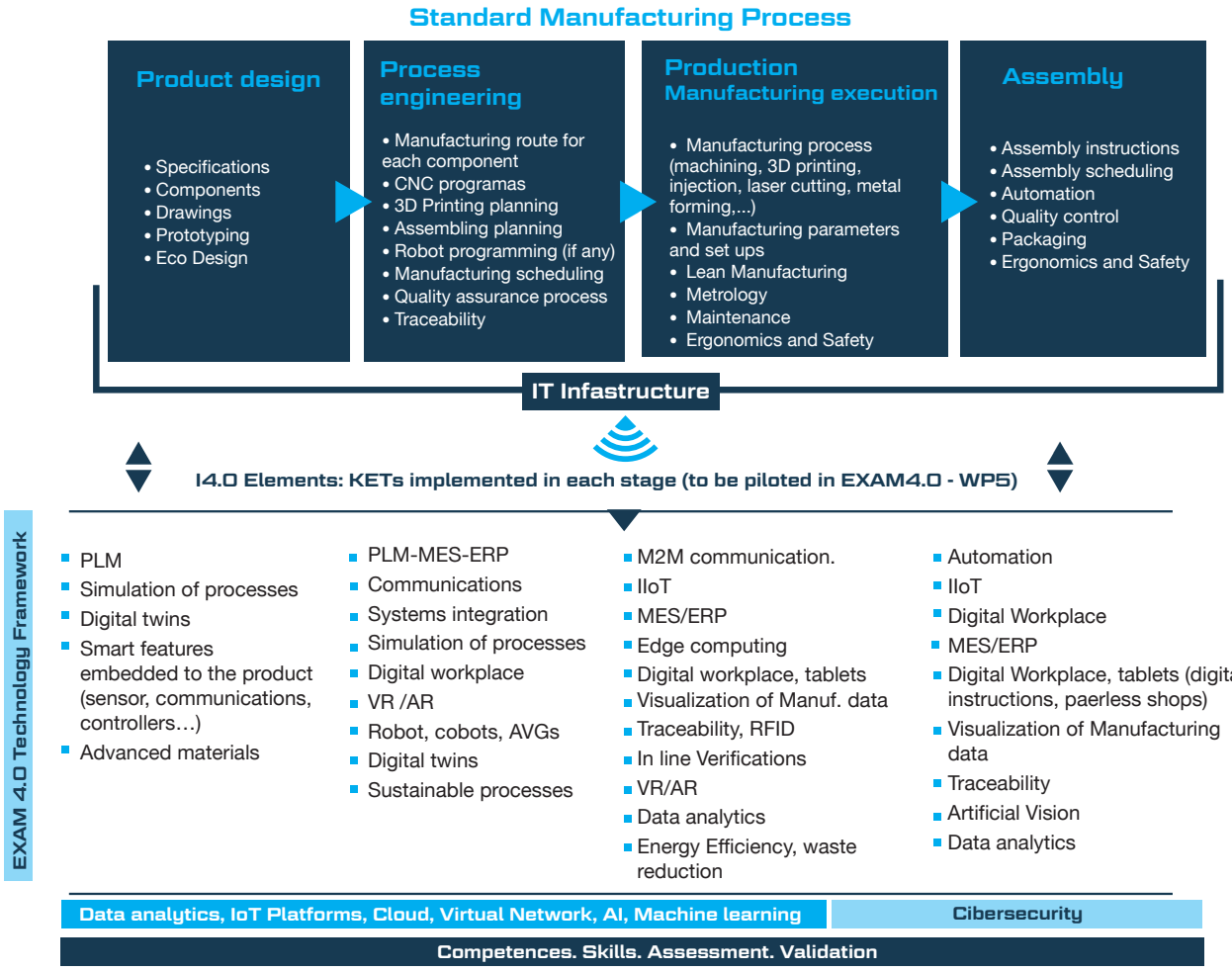

Figure 6: EXAM4.0 Collaborative Learning Factory's (CLF) Value Chain Source:Author's creation

The previously mentioned Cybersecurity scenarios will be useful in all the stages of the CLF.

In early stages while the student makes the analysis and design is done, all the components such as firewalls, servers… and subnet design among other things must have a place.

In mid-late stages cybersecurity will provide a more quiet environment, with less risk, never being 0 risk. Due to this, cybersecurity protocols and systems should be checked and improved constantly.

This focus on cybersecurity will ensure that the students enrich their profile with these capabilities. In order to achieve this, we will design several teacher training programs focused on VET teachers, allowing them to add this knowledge in their previous subjects.

2.3.Benefits of using cybersecurity in EXAM4.0's CLF

There are huge benefits to adopting and integrating Cybersecurity in the EXAM CLF.
These are some of them:

- Risk awareness
- Improve security
- Gain risk detection and management capabilities
- Simulate attacks in a controlled environment
- Improve reaction time against real attacks
- Test of different network compositions to make sure that is secure
- Development and Research of new attacks to industrial components and different systems such as RFID, NFC...

The greatest benefit of Cybersecurity is that it provides the skills to identify the risks in both IT and OT scenarios, and therefore help to create secure CLFs. And of course, all these benefits are directly transferred to the students.

2.4. Competences addressed with cybersecurity

The competencies acquired with data analytics can be classified into two groups: Technical and soft competences.

The technical competences are the ones that are most closely related to the technical content to be acquired in the learning process of the students.
Among other technical competences the main ones are:

- Knowledge about Cybersecurity technology
- Cybersecurity risk assessment
- Cybersecurity Monitoring and Reporting
- Vulnerability and Penetration Testing
- Creative thinking
- Secure software development
- Fundamental skills about how to use IT tools securely
- Secure configuration of IT and OT infrastructure

As for the soft competences developed with cybersecurity are:

- **Teamwork:** being a collaborative tool, team members can plan their tasks and all have access to the production sheets, the control sheets....
- **Digital awareness:** they get used to virtual working environments, understanding the data obtained, managing it and drawing conclusions.
- **Personal:** autonomy, initiative, critical spirit, to be aware of the importance of good p**lanning and to see how the decisions taken in the process affect them.**
- **Communication:** between different students, the one who plans the production with the one who executes it, being aware of the importance of the different explanations (verbal and written) that are given within the production process and that can help achieve a better result

3 Collaboration opportunities opened by cyber-security

The knowledge acquired with the different Cybersecurity scenarios empowers the HVET users not only to create secure remote collaboration opportunities from other laboratories interested in the same field, but also to promote them to test theoretical knowledge into real scenarios.

In a similar way, collaboration with non-academic institutions is very important. External partners and enterprises can provide with real life scenarios that need to be addressed and tested on the CLF, as nowadays cybersecurity is not optional but a requirement.

4 References

Wikipedia. (25 October 2021). Retrieved from https://en.wikipedia.org/wiki/Computer_security

EXAM 4.0

THE EXCELLENT ADVANCED MANUFACTURING 4.0