Path towards embedding industry 4.0 paradigm – Digital competence overview in HEI: The Alto Minho Region case study

T Pereira, A Amaral and L Barreto

1 Escola Superior de Ciências Empresariais (ESCE), Instituto Politécnico de Viana do Castelo (IPVC), Avenida Pinto Mota Valença, Portugal
2 Instituto Superior de Engenharia do Porto (ISEP), Instituto Politécnico do Porto, 4249-015 Porto, Portugal

*Corresponding author: tpereira@esce.ipvc.pt

Abstract: The increased adoption of IoT and analytical devices, telecommunication systems, smart sensors, and diverse information systems have brought significant impacts to Industry 4.0. To respond to this rapid technological evolvement is essential to ensure a proper articulation of HEI (Higher Education Institutions) with industry, to better prepare graduates with the appropriate competencies and technological capabilities within the digital transition of the industry. This paper aims to present a research project developed in digital transformation amongst HEI students, in the Alto-Minho region disclosing the trigger points to increase the digital adoption and embedding of Industry 4.0 paradigm. The obtained results enabled to conclude an apparent low level of digital literacy, a lack of vision and awareness about the technology potentialities throughout industry activities, besides its use almost restricted to leisure and as study support, as well as lack on cybersecurity domain-specific competencies.

Keywords: Industry 4.0, Digital literacy, Cybersecurity, Digital competencies, Human disposition or abilities.

1. Introduction

Industry 4.0 paradigm is deeply associated with the use of interconnected drones, robots, smart security devices, autonomous vehicles, meaning business and industries that foresee Industry 4.0 rely more and more on digital technologies such as intelligent devices, IoT devices, telecommunication systems, smart sensors, analytical devices, and big data. However, as stated by [1] “In Industry 4.0, people are the key players — work is getting easier, safer and more efficient — enabled through technology — but machines will continue to play the subordinate role”. With such a level of digital transformation [2] and digitalization and being people essential for the development of such businesses, Higher Education Institutions (HEI) also have an important role as their graduate students will have to play key roles in those businesses. Today’s students will be the future workforce, thus will need to work in an increasingly interconnected world, under more distributed and digital business models, and will be expected to collaborate with peers using digital tools to enable these new types of interactions. In this context, it is important to analyze HEI available curricula [4] and assess the graduates’ level of competencies towards being digital-ready [5]. With that sense, this paper aims to present a research project developed about
digital transformation amongst HEI students, in the Portuguese Alto-Minho region, disclosing the trigger points to increase the digital adoption and embedding of the Industry 4.0 paradigm.

The paper is organized as follows: in the next section, Section 2, it is presented the Industry 4.0 challenges and an overview of the workforce competencies. Section 3 presents the developed research performed on the Alto-Minho HEI’ students and the survey results. Based on the survey results, it is presented in Section 4, an analysis of the cybersecurity domain-specific competencies within Industry 4.0. Finally, Section 5 presents the conclusions and future work to the presented research performed.

2. Overview of the Industry 4.0

2.1. Industry 4.0 Challenges
The technological advances contributed to the digital transformation processes not only in industry 4.0 but also in the public sector and thus in HEI curricula offers.

Figure 1 presents the Industry 4.0 challenges developed by the research project: Universities of the Future (UoF) [5].

![Figure 1. Challenges of Industry 4.0, source from [7].](image)

The UoF project researchers clearly identified, within the Industry 4.0 development, the following challenges: 1) the lack of strategy to prepare the future work; 2) the lack of skilled workforce and 3) the lack of vision on technology [5].

These challenges emphasize the impacts the technological resources and the lack of time efficiency have on the way people work, especially concerning their daily tasks’ management development, their understanding of the context possibilities, and the efficient use of the available digital tools.

The work is no longer restricted to a place or time. The rapid evolvement of technological resources should be aligned with the capacity to envision future work. The main challenge is to understand how future work could be like; what organizational support structures are necessary; and the type of legislation and regulation required to be developed to support it.

The lack of a skilled workforce, negatively affects businesses, performance, and productivity, compromising innovation with higher impacts on human lives and environmental sustainability. Unequal access to education and technological learning resources influence competition. Resistance to change also slows down people’s involvement to create new curricula as well as the motivation to enrol in new programs.
Lastly, the lack of vision on technology is related to the inability to understand the potential use of technological resources, not only in the work performance but also in its impacts on people’s life and the environment. The lack of a skilled workforce is the main cause of the lack of insight into the technology, compounded by people’s resistance to change, tending to focus on one point of view, rather than looking at the whole scenario. Altogether, leverage the right technology investments hindering the systems integration and consequently the implementation of Industry 4.0 [5].

Additionally, the rapid evolvement of Industry 4.0, the widespread and the emergence of the technological resources available, and their quick adoption in the industrial operational processes, trigger’s the hackers’ appetite for the exploitation of their inherent vulnerabilities, aiming to perform one or more cyberattacks with critical operational and financial impacts. The integration of new systems and their increased hypothetical potential third-party access, enlarge the cybersecurity risks challenges. Therefore, cybersecurity must be emphasized as a critical issue in the digital transition and to the success of Industry 4.0. It is important to ensure the protection of the critical industry infrastructures as well as the data and information contained in their systems against misuse and unauthorized access [4]. In this context, the cybersecurity knowledge and its good practices, will be an important challenge to be considered within the scope of Industry 4.0.

Focusing on the cybersecurity risks and the second Industry 4.0 challenge, regarding the lack of a skilled workforce, the following subsection introduces a brief overview of the European digital competencies.

Figure 2. Results of the human basic digital skills. Source: Digital Economy and Society Index Report 2020 – Human Capital, European Commission [6].

2.2. Overview on Workforce Digital Competences

The European Commission provided a report analysis on ICT skills named “Digital Economy and Society Index 2020 Human capital” [6], presenting the evolvements on the Internet users skills (at least basic skills) and advanced skills (ICT graduates and ICT specialists). These skills are presented into the following dimensions: 1) information skills (indicators’ examples such as: copy or move files or folders, access to information from public authorities/services’ website, et cetera); 2) communication skills (indicators’ examples such as: sending/receiving emails, uploading self-created content to any website to be shared, et cetera); 3) problem-solving (indicators’ examples such as: transferring files between computers or devices, connecting and installing devices, installing a new or replacing an old operating system, et cetera) and 4) content creation (indicators’ examples such as: use of word processing and use spreadsheets software). An additional skill named “Safety” was also considered, but not presented due to a lack of appropriate indicators available. Furthermore, basic and advanced skills’ indicators are identified and listed in the former draws on the European Commission’s Digital Skills Indicators [6].

Figure 2 presents the human capital indicators in the Digital Economy and Society Index [6]. This figure evidences the slow evolvement of digital skills, and although the increase robustness of
the ICT infrastructures [5], the increased 85% of citizens that use the Internet in 2019, prior to the COVID-19 pandemic, it can be concluded that only 58% possesses at least basic digital skills [6].

These results clearly sustain the workforce’s lack of digital competencies in Industry 4.0, reinforcing the continuous need for investments in ICT competences, but also emphasising the urgent need to go forward and raise discussion on extending or even including cybersecurity competencies, within the Industry 4.0 challenges.

3. Research Study Performed

The rapidly increasing and continuous transformation of processes’ digitalisation and the evolvement of Industry 4.0 enforces the creation of innovative educational offers and resources. It seems that learning how to learn is gaining a different perspective within this new context that needs to be fully captured throughout the digital transformation, which creates outstanding conditions to change the learning paradigm as well as establishing the purposes for its evolvement. It is also extremely important to combine the market’s dynamism throughout the value chain with the driving forces for Industry 4.0 implementation [6].

To address these educational needs and to diagnose them, a survey was developed towards detecting and understanding the level of competencies and skills. The developed survey was divided into 3 groups of questions. The first group included questions aimed to identify the socio-demographic characterization, including the basic information (gender; age; course graduation and domain of study; et cetera). The second group of questions intended to assess the number of technological gadgets and tools the graduates own and for which purpose they use them. The last group of questions aimed to assess the graduate’s awareness of cybersecurity threats. In the context of the digital transition, this part of the survey aimed to compare the use of technological gadgets and tools with graduate’s awareness about cybersecurity risks. The survey was shared with HEI graduates from the Alto Minho region of Portugal and 95 responses were obtained. A summary description of the survey respondents’ is followed presented accordingly the 3 groups of questions.

Analysis of the socio-demographic characterization

- The female gender had more active participation than the male gender.
- Most of the respondents were from 20-25 years old, followed by 17-19 ages.
- The geographical location of the respondents was from 15 Portuguese districts. The highest number of respondents were from Viana do Castelo district with 48 participants, followed by Porto, with 10 respondents. This number might be related to the fact the authors of this study are researchers of Polytechnic Institute of Viana do Castelo, geographically located in the Alto Minho region of Portugal.
- The highest number of respondents have their permanent residence on cities like Valença, Viana do Castelo, Vila Praia de Âncora, Melgaço, Viseu and Chaves (North and West of Portugal). While from the South and Center, the respondents were mainly from the cities of Lisboa, Sintra, Elvas, and Albufeira.
- The graduates’ participation is mainly from graduation studies, followed from master and postgraduate studies.
- The studies’ area of the respondents is mainly from Social Sciences, Commerce and Informatics, followed by Services and Health, and Social Protection.

Analysis of the technological devices use

- The devices the graduates widely use are the laptops, followed by the smartphones and tablets;
- Above 50%, the usability of these devices is mostly used in social networks; to perform research on the Web and mainly to access information to support the graduates’ studies, to read economic and financial news, access lifestyles and celebrities’ information, and read local journals; email applications; office applications and to download and read information. Bellow 50%, the
devices are used to access collaborative tools, to listen to music, and lastly to access and use the ERP tools. The graduates consider the use of technologies highly contributes to better understanding the subjects, to easily organize their study, to enable a greater study autonomy, and to turn it more interesting and enjoyable. The less favourable results are related to the reduction of human relations and interaction with the teacher and colleagues, easily loss of attention, decrease attendance to classes, and difficulties to manage the amount of information.

Analysis of graduate’s awareness about cybersecurity risks.

- All the graduate participants are, somehow, aware of their greater exposure to cybersecurity threats when they use technology and are online.
- A lack of knowledge about cybersecurity policies and secure good practices. The cybersecurity policies implemented by less than 50% of the graduates are limited to Software (SW) update because it can be automatically configured, backups implementation, followed by the implementation of password management. Only 53% of the graduates implement antivirus and firewalls.
- 41% of graduates recognize to have a reduced knowledge of cybersecurity protection mechanisms and their current knowledge was gained by self-learning, while 24% gained it by active learning with a teacher and 22% with friends and colleagues.
- A complete lack of skills to manage cybersecurity risks.

4. Discussion and Survey Results
Graduates recognize the evolvement of the digital transformation processes in the industry, higher education institutions, and broadly in the public sector. An interesting and important result of the survey was the lack of vision on technology by the students. They foster technology more as a leisure option and a study complement, without really understanding its potential use and the impact that it can cause for work and other activities. Students also show an inability to choose and invest in the right technology as well as an inability to achieve broader use and integration of it.

Another conclusion from the survey is that students’ investment is higher in new and sophisticated technological devices rather than in cybersecurity protection (awareness training initiatives). This results in a less preventive and awareness culture, and consequently in a more reactive attitude towards cybersecurity threats and attacks. Students are aware of cybersecurity risks but perceive a lack of cybersecurity competencies highlighted by their pursuit of self-learning. This requires HEI actionable actions to assess their curricula, by redefining them in terms of main goals, skills, and attitudes, creating innovative educational offers and resources, and give strategic directions and insights to prepare graduates for the Industry 4.0 challenges.

5. Challenges of The Cybersecurity workforce’ Literacy Challenge within Industry 4.0
Accordingly, to the results presented in the previous section and the studies developed in this domain, it is recognized a gap of digital competencies on Industry 4.0, enlarged to the lack of cybersecurity good practices competencies to respond to the widespread number of attacks aimed to compromise the operability of the industry/organizational processes. Digital cybersecurity can only be ensured with a workforce prepared with the right knowledge, skills, and human dispositions (human attributes, attitudes or abilities) [7].

Knowledge includes formal compulsory education and also informal and non-formal learning, outside of compulsory education; human disposition requires critical thinking, problem-solving, communication, collaborative network, legal and ethical principles [8]. Parrish et al., reinforce this assumption suggesting that “competency is some combination of knowledge, skill and ability” [7]. Further, the MSIS2016 document [8] states: “Competences represent a dynamic combination of cognitive and meta-cognitive skills, demonstration of knowledge and understanding, interpersonal, intellectual and practical skills, and ethical values.”.
For example, having knowledge about a programming language does not make anyone a good software developer; being a good programmer is a skill, not a competency; being a good communicator is a human ability, not a competency. Figure 3 illustrates this understanding in the context of information technology, where the intersection of the concepts – knowledge, skills, and human disposition - describes the intended competency.

Figure 3. Competency intersection of the concepts Knowledge, Skills and Disposition, source [7].

Based on these concepts and in the obtained survey’ results, some inferences could be presented:

1. Graduates use technologies to support and organize their studies as well as a facilitator to have a greater study autonomy, but it is recognizable a lack of skills to manage huge amounts of information; further, a reduced attitude/human disposition to communicate and to have better human relations between teachers and colleagues.
2. Graduates have the knowledge and are, somehow, aware of the cybersecurity threats and their major impacts, but they recognized a lack of cybersecurity protection skills; self-learning and capability to communicate with colleagues are attitudes/human disposition factors to improve their competencies in cybersecurity protection.
3. Graduates point out they have limited knowledge about cybersecurity policies (antivirus, firewalls, SW updates, password management) but recognize their lack of skills when protection technologies demand specific configurations, instead of automatic configurations.
4. Graduates are, somehow, aware of their great exposure to cybersecurity risks when they use technology or are online but recognize a complete lack of skills and adequate attitudes/human disposition to manage cybersecurity risks, including cybersecurity risk considerations in creating an effective cybersecurity project plan.

These results enable to sum up the following assumptions: 1) improving skills and knowledge promotes motivation thus better attitudes/human disposition to achieve new additional competencies; 2) increasing cybersecurity knowledge will encourage dynamic attitudes to foster entrepreneurial initiatives in digital literacy; 3) cybersecurity awareness requires skills in cybersecurity threats and attitudes/human disposition for security good practices; 4) training graduates in knowledge and attitudes/human disposition towards the context (digital manufacturing; supply chain management; cyber-physical systems, IoT, et cetera) can improve skills by increasing digital literacy for more technical domains, lastly although the context, the adequate competencies must always focus in the intersection of the concept’s knowledge, skills, and human dispositions.

These achievements enforce the HEI’s challenge in reshaping their curricula and ensuring the adequate level of competencies (what graduates know and can do by the time they graduate) on the
professional practice domain, thus narrowing today’s digital competencies gap with the competencies expected by employers. Furthermore, it is fundamental to develop joint efforts between HEI with industry to understand their present and future digital needs. However, in the Portugal context, a steady ICT infrastructure is developed and a high number of STEM (Science, Technology, Engineering, and Mathematics) graduates, but the industry still has difficulty finding staff with those competencies [5]. This difficulty is experienced by many SMEs in Portugal. Consequently, the industry does not have the financial capacity to hire a cybersecurity specialist, and at the same time a database manager, a network and communication manager, etc. In Portugal, most industries and organizations hire one IT specialist to ensure all these tasks. One strategy of the SME is providing training to their IT staff, but most of them demand to their IT staff a self-learning initiative. This has serious impacts not only on the efficient performance of the IT staff, but also on their personal and family lives, negatively affecting businesses. This context partially justifies the difficulties from HEI to articulate their curricula towards the industry digital needs. However, HEI must also embrace new models, such as School as a Service (SaaS) [9], towards working in a collaborate and multidisciplinary manner, allowing to combine different realities and sensibilities, to define models that can emphasize the Industry 4.0 workforce competences needs [10]. The SaaS approach is more a student-centered philosophy than a teacher-centered one, creating a unique student profile, thus allowing to have customized learning for every student and promoting the competency-based learning environment measured by multiple assessments as part of learning experiences. With SaaS, it is possible to create open industrial experiences [11], enriched with gamification [12], simulations [13], and intelligent learning environments [14], tailored-made for every student and with the ultimate goal of potentiating Industry 4.0 competencies.

Accordingly, to [15], the IMS-based model levels for smart manufacturing adoption, it is critical the adequate management commitment and financial support as well as the definition of a strategic roadmap for digitalization. This will be of capital importance to mitigate the barriers of the digital transformation adoption within companies and the alignment between the competencies evolution through time towards ensuring the digital literacy and the organizational readiness level [15]. Simultaneously, it is noticeable the projected gap between the cybersecurity competencies gained throughout the HEI curricula and the higher level of maturity presented that deals with operations technology and cybersecurity.

6. Conclusions and Future Work
The technological evolvement risen from the Industry 4.0 demands to the HEI the assessment of their curriculums in terms of its main goals and competencies towards embedding Industry 4.0.

The research work developed enables to gain insights on graduates’ vision and awareness towards digital transformation, contributing as future work the assessment of the HEI curriculums and support the reformulation of those same HEI curricula in terms of main goals and competencies. It also confirms the misalignment between industry and the HEI and how this is critical to overcoming the huge gap that is already being felted. New learning content and new methodologies must be considered towards ensuring future professionals contribute to building growing and inclusive economies, especially in smaller and poor regions, like the Alto Minho region.

The cybersecurity pillar of Industry 4.0 will be of capital importance to ensure the overall confidence of all the stakeholders within the digital transformation ecosystem. Therefore, an intelligent systems design should be incorporated to avoided and limit the users’ risky behaviour thus ensure higher levels of security. Furthermore, the development of an AI algorithm to detects risk patterns and suggests users’ ways to avoid them, as well as pointing alerts to its potential consequences and impacts could be a technological strategy to consider. Finally, the HEI curricula development dynamism should embed the SaaS paradigm towards being able to actively evolve in a seamless, systemic, and holistic manner.

Acknowledgements
Teresa Pereira acknowledges the support by Applied Digital Transformation Laboratory (ADiT-LAB) research center of IPVC and FCT – Fundação para a Ciência e Tecnologia within R&D Units Project.
Scope: UIDB/00319/2020”.
Luís Barreto also acknowledges the support by the ADiT-LAB research center of IPVC.

References

[1] Santos M Y et al. 2017 A Big Data system supporting Bosch Braga Industry 4.0 strategy. *International Journal of Information Management* **37** (6) pp 750–760

[2] Vial G 2019 Understanding digital transformation: A review and a research agenda *The Journal of Strategic Information Systems* **28** (2) pp 118–144

[3] Durek V, Kadoic N and Begicevic N 2018 Assessing the digital maturity level of higher education institutions *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (Opatija, Croatia)* pp 671–676

[4] Khan N and Forshaw T 2017 Available at: https://www.accenture.com/t20171011T185302Z__w__/us-en/_acnmedia/PDF-63/Accenture-New-Skills-Now-Inclusion-in-the-digital.pdf

[5] Pereira T, Barreto L and Amaral A 2017 Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing* **13** pp 1253–1260

[6] Universities of the Future, 2020. Blueprint for the Universities of the Future. *Erasmus+ Programme of European union* (https://universitiesofthefuture.eu/wp-content/uploads/2019/08/Briefing-Blueprint-UoF.pdf.)

[7] European Commission 2020 Human Capital and Digital Skills. Shaping Europe's digital future (https://ec.europa.eu/digital-single-market/en/human-capital-and-digital-skills) accessed 4 March 2021

[8] Parrish A, Impagliazzo J, Raj R K, Santos H, Asghar M R, Josang A, Pereira T, Sá V J and Stavrou E 2018 Global perspectives on cybersecurity education. *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (Larnaca Cyprus)* pp 36–54

[9] Topi H 2017 IS EDUCATION 2016: guidance and inspiration for master's programs in information systems *ACM Inroads* **8** (2) pp 27–28

[10] Vladykina N, Uribe A C and Ahlava A 2019 School as a Service: Platform for Learning in Upper Secondary Education operating on Aalto University Campus *Proceedings of the 5th IEEE International Smart Cities Conference (ISC2) (Casablanca, Morocco)* pp 303-309

[11] Trotta D and Garengo P 2018 Industry 4.0 key research topics: A bibliometric review *2018 7th International Conference on Industrial Technology and Management (ICITM) (Oxford, UK)* pp 113-117

[12] Weissenberger-Eibl M and Koch D J 2007 Importance of industrial services and service innovations *Journal of Management & Organization* **13** (2) pp 88–101

[13] Kim S, Song K, Lockee B and Burton J 2018 What is Gamification in Learning and Education?. *Gamification in Learning and Education. Advances in Game-Based Learning* (Springer Cham) pp 25–38

[14] Tvenge N and Martinsen K 2018 Integration of digital learning in industry 4.0 *Procedia Manufacturing* **23** pp 261–266

[15] Desmarais M and Baker R 2012 A review of recent advances in learner and skill modeling in intelligent learning environments *User Modeling and User-Adapted Interaction* **22** (1-2) pp 9–38

[16] Ghobakhloo M (2020) Determinants of information and digital technology implementation for smart manufacturing *International Journal of Production Research* **58** (8) pp 2384–2405