Issues in Information Systems
Volume 25, Issue 3 pp. 148-164, 2024

DOI: https://doi.org/10.48009/3_iis_2024_112

Transforming industries: the digital revolution of industry 4.0

Olena Kulykovets, *Warsaw University of Life Sciences, olena_kulykovets@sggw.edu.pl*

Abstract

The evolution of industry, marked by significant technological advancements and the integration of digital innovations, has ushered in the era of Industry 4.0. This paradigm shift, characterized by the convergence of cyber and physical systems, presents both challenges and opportunities for businesses across various sectors. This article explores the multifaceted landscape of Industry 4.0, beginning with its historical context and progression through the stages of digital transformation. Emphasizing the pivotal role of smart manufacturing and the Industrial Internet of Things (IIoT), the study highlights the potential for increased efficiency, productivity, and customization in production processes. However, the widespread adoption of digital technologies brings forth cybersecurity concerns, necessitating robust measures to safeguard data and systems. Despite challenges, the global smart manufacturing market is poised for substantial growth, reflecting the increasing demand for intelligent solutions. The article examines variations in regional adoption of Industry 4.0 technologies in the European Union (EU) and outlines policy recommendations to foster digital transformation. Furthermore, the study underscores the importance of digitalization for small and medium-sized enterprises (SMEs) and outlines targets set forth by the European Commission to promote digital technology integration by 2030. Industry 4.0 represents a paradigm shift with far-reaching implications for businesses, economies, and societies. Embracing digital transformation, while addressing associated challenges, is imperative for staying competitive in an increasingly interconnected world.

Keywords: Industry 4.0, Cybersecurity, Digital Transformation, Smart Manufacturing, Digitalization of SMEs, European Union (EU) Policies, IoT (Internet of Things)

Introduction

Industry is the part of the economy that is responsible for the production of material goods. Since the beginning of industrialization, the technological leap has led to changes that are today called the "industrial revolution": in the field of mechanization (I industrial revolution), intensive use of electricity (II industrial revolution) as well as widespread digitalization (III industrial revolution) (Lasi et al., 2014). In the 21st century, shorter product life cycles and increasing consumer demands pose many production challenges, and unsustainable resource use practices can limit production.

The current universe is experiencing a revolution where the processes and tools of the physical world are being transformed into a digital version. The rapid development of smart devices and new technologies has enabled humanity to constantly communicate at anytime and anywhere. The manufacturing industry is one of the key sectors that has a huge impact on the economy and development of the entire country (Sahoo & Lo, 2022). Modification of production processes as well as improvement of efficiency, and at the same time, product quality are the basis for the functioning of the economy. Therefore, new technologies, now popularly called "intelligent production", are constantly being developed (Kusiak, 2017). This technology

plays a key role in achieving better results with reduced human workload, increased quality and durability of production activities and lower costs. The trend Internet of Things (IoT, Internet of Things) has created the foundations for the emergence of the subsegment of the industrial Internet of Things, commonly called Industry 4.0 (Munirathinam, 2020). Industry 4.0 introduces decentralized control through networked intelligent systems that enable self-regulating production where people, machines, devices and products communicate with each other (Gubán & Kovács, 2017). Moreover, the intelligent production process, entering the trend of the Internet of Things, creates conditions for cooperation in communication between machines and products, taking into account information collected directly from the customer (Yang et al., 2019). Smart manufacturing is the full integration and execution of all aspects of production processes through the use of a data-driven, understandable, planned, and organized model supported by advanced sensing, simulation and analysis technologies that can respond in real time to keep up with constantly changing requirements and conditions prevailing both within the company, in the supply chain and consumer needs (Lu et al., 2020). The ultimate goal of smart manufacturing is to meet consumer needs for personalized and environmentally friendly goods and services (Moghaddam et al., 2018).

According to a report by the McKinsey Global Institute, approximately 60% of all professions available on the market have at least 30% of activities that can be completely automated, thus showing that the effective use of intelligent production technologies can contribute to the increased production capacity of intelligent enterprises (Manyika, 2017). The COVID-19 pandemic had a significant impact, especially on the production sector, which in turn forced manufacturers to implement solutions provided by intelligent production. With increasing demand for both everyday and electronic goods, the global smart manufacturing market is expected to witness significant growth in the coming years. Moreover, the global market for this production is expected to increase from USD 249.46 billion in 2021 to USD 576.21 billion in 2028 with a compound annual growth rate (CAGR) of 12.7% (Fortune Business Insights, 2024).

The main purpose of the article is to explore the evolution and current state of Industry 4.0, highlighting its transformative impact on industrial production. It aims to demonstrate how smart manufacturing, enabled by technologies like the Industrial Internet of Things (IIoT) and cyber-physical systems, enhances production efficiency, quality, and responsiveness to market demands.

The article discusses the evolution of the industry through different revolutions and emphasizes the current transformation into Industry 4.0. The methodology in this article used to be a literature review combined with analysis and synthesis of data from various sources, including reports, surveys, and institutional documents. Firstly, it provides a historical overview of industrial revolutions and their impact on production, setting the context for the emergence of Industry 4.0. Then, it delves into the core concepts of Industry 4.0, such as smart manufacturing, cyber-physical systems, and the Industrial Internet of Things (IIoT), explaining their principles and implications.

The text employs statistical data to illustrate the current state and projected growth of Industry 4.0, providing quantitative evidence to support its claims. Furthermore, it discusses the adoption of Industry 4.0 technologies across different sectors and countries, analyzing variations in implementation levels and identifying challenges and opportunities. The article also involves policy analysis, where it examines the strategies and recommendations proposed by institutions like the European Commission. Lastly, it integrates examples to illustrate the practical implications of Industry 4.0, such as its impact on cybersecurity, economic development, and digital transformation within businesses. Overall, the methodology of this article combines theoretical frameworks, empirical data, and policy analysis to provide a comprehensive understanding of the evolution and implications of Industry 4.0.

Issues in Information Systems
Volume 25, Issue 3 pp. 148-164, 2024

Foundations of Industry 4.0: From Cyber-Physical Systems to Smart Manufacturing

Germany is the pioneer of the fourth industrial revolution, called Industry 4.0. The promotion of computerization of the production process began in 2011. The basis of Industry 4.0 is cyber-physical systems (CPS), which focus on machine learning, real-time data processing and connectivity of various elements. In practice, this means that machines interact by connecting the Internet of Things (IoT) and the industrial Internet with the production system to share information in real time. The associated system algorithms support intelligent decision-making during the production process. Artificial intelligence, rapid prototyping, flexible production automation systems and augmented reality have been widely used in the fourth industrial revolution (Zhang & Yang, 2020). Most countries have already introduced their policies regarding the implementation of cyber-physical systems (CPS) and digital manufacturing in the near future (Arnold et al., 2016). The implementation of new solutions in the Industrial Revolution 4.0 is a gradual process because it requires time and a lot of commitment to update existing systems. Physical infrastructure, adoption of new technologies, knowledge transfer, availability of technical labour and security are some of the numerous challenges of enterprise modernization to adapt to modern Industry 4.0 systems (Phuyal et al., 2020).

Industry 4.0 basically consists of three stages:

- Stage one – obtaining digital records using sensors connected to industrial assets that collect data by accurately mimicking human feelings and thoughts. This technology is described in the literature as sensor fusion;
- Second stage – analysis and visualization including the implementation of analytical capabilities on aggregated data using sensors. From signal processing to optimization, visualization and cognitive computing, activities often take place in the background. The operating system is supported by an industrial cloud, which supports the process of managing very large amounts of data.
- Third stage - translating insights into concrete actions by transforming aggregated data into meaningful results such as prototyping (additive manufacturing), autonomous robots, digital design and simulations. In the industrial cloud, raw data is processed using a data analysis tool and then transformed into practical and useful knowledge (Ervural & Ervural, 2018).

The term Industry 4.0 covers a variety of concepts that are difficult to classify and distinguish. It includes smart factories based on digital technology; cyber-physical systems, combining the physical and digital levels; growing self-organization of production systems; new approaches to distribution and supply and the development of products and services; the need to adapt production to human needs; and the increasing importance of corporate social responsibility. These concepts lead to a more individualized approach to both production, distribution and product development, while considering ecological and social aspects (Lasi et al., 2014).

However, although Industry 4.0 is still primarily associated with manufacturing, some definitions apply to other industries, suggesting that Industry 4.0 concepts can be used to characterize the technological evolution of other activities beyond manufacturing (Culot et al., 2020a). New ideas and technologies may make the boundaries between different industry sectors less clear. This process is supported by institutional strategies that do not focus solely on production, and by the involvement of both manufacturing and service companies in creating joint offers that integrate diverse products and services (Weber & Schaper-Rinkel, 2017).

Industry 4.0 is also about combining technologies, machines, and integrated processes with production procedures throughout the supply chain and value chains, supporting self-sufficient production processes

and decisions made with minimal human involvement. This integration is made possible by consistent and flexible communication and computerization, which enables greater automation, and production systems capable of self-adaptation, which in turn allows for autonomous and decentralized decision-making (Hofmann & Rüsch, 2017). More broadly, Industry 4.0 can be identified as a set of disruptive technologies that are changing the way companies across all industries plan, execute and evaluate their business strategies (Culot et al., 2020b).
Non-manufacturing sectors are adapting to the execution capabilities of Industry 4.0 at different rates and with different impacts. The transportation and logistics as well as wholesale and retail industries are closely related to supply chain operations, so they take advantage of the integration opportunities offered by Industry 4.0 technologies. IoT, CC, AM and BDA enable the integration of the supply chain and production processes, which facilitates planning and minimizes disruptions, thereby increasing the resilience of the entire supply chain (Ben-Daya et al., 2019). Automatic identification technologies such as radio frequency identification (RFID) tags and readers, cloud-based enterprise resource planning (ERP) systems, blockchain and CPS enable access to real-time demand information (Barreto et al., 2017). Trade development, both on a larger scale and at the retail level, benefits from the use of smart tags. In addition to the popular QR codes, barcodes and RFID labels that are used to manage inventory, Internet of Things technology opens up new opportunities to add additional information for communication with smart factories or can simply be read by customers using e.g. mobile phones (Fernandez-Carames & Fraga-Lamas, 2018).

The Industrial Internet of Things (IIoT) has the potential to radically change the future, impacting industrial systems and the lives of many people, offering them the opportunity to improve their careers, and living standards. Realizing the full potential of IIoT will lead to intelligent solutions in various fields such as healthcare, logistics and diagnostics, also will enable the development of smart factories, and autonomous systems as part of Industry 4.0. Thanks to these innovations, it is possible to achieve an unprecedented level of operational efficiency and productivity growth by introducing advanced production processes based on human-machine cooperation. The Industrial Internet of Things has a promising future, but a key challenge is data security and privacy, which could limit its potential if not addressed effectively. It is necessary to focus on countering cybersecurity threats and remove obstacles for those implementing industrial IoT technologies to fully realize the benefits of this technology (Thames & Schaefer, 2017).

In the context of Industry 4.0, cybersecurity is crucial for maintaining companies' competitiveness (Lezzi, et al., 2018). Manufacturing systems in the past were self-contained, with security maintained through their isolation and controlled physical access. Nowadays, however, contemporary manufacturing equipment is outfitted with numerous intelligent devices (such as sensors and actuators) and is interconnected with other machines and data processing systems through wireless networks or wired Ethernet. These manufacturing elements interact over private industrial networks using specialized protocols, but these protocols do not offer sufficient protection against cyber threats (ENISA, 2018). Currently, critical industrial equipment is susceptible to various cyber-attacks that can impact the entire business model. According to Cisco's 2018 Annual Cybersecurity Reports (Cisco, 2018), 31% of organizations have encountered cyber-attacks on Operational Technology (OT), and 38% anticipate that attacks will shift from Information Technology to Operational Technology. Despite 75% of experts recognizing cybersecurity as a priority, only 16% believe their company is adequately prepared to handle cybersecurity challenges (Bauer et al., 2017).

Challenges in Industry 4.0 for Enterprises

Increased data density within Industry 4.0 as well as the fusion of information and operational technologies brings with it many challenges, especially in the field of cybersecurity (Frost & Sullivan, 2017). Cybersecurity involves protection against abuse, unauthorized access, or theft of both business information

and valuable knowledge about an item or system. With the rapid development of network connections, cyber-attacks have become more common due to the increasing tendency to misuse data for various purposes, including strategic or financial considerations (Ervural & Ervural, 2018). Moreover, cybersecurity plays a key role in maintaining a high level of enterprise competitiveness. Today, critical industrial equipment is exposed to several threats related to cyber-attacks, which, by the way, can have a very large impact on the entire business model of the company (Lezzi et al., 2018). According to Cisco's 2018 Annual Cybersecurity Reports, approximately 31% of enterprises have experienced cyber-attacks on operational technologies during their operations, while 38% of organizations expect cyber-attacks to be carried out not only on operational technologies but on all units of the technology pipeline. Although 75% of experts perceive enterprise cybersecurity as a priority, only 16% confirm that their organization is well-prepared for a potential cybersecurity crisis (Cisco, 2018). The European Cybersecurity Organization (ESCO), as part of the European Digital Single Market, created one document in 2017 which collected all existing standards and specifications related to cybersecurity. The main goal of such activity was to create a document that would help understand and select appropriate schemes that can be used by enterprises to meet the challenges related to cybersecurity (ECSO, 2017). Moreover, the International Electronic Commission (IEC) has published a guide on information security and data privacy to be covered in IEC publications and explains how to implement them. This publication constitutes recommendations (accepted by the IEC National Committees) for international use (IEC, 2018).

The National Institute of Standards and Technology (NIST) defines a cyber threat as "any circumstance or event that may adversely affect an organization's operations (including mission, functions, image or reputation), an organization's assets, persons, other organizations, or the nation through a system information through unauthorized access, destruction, disclosure, alteration of information and/or denial of service" (NIST, 2013). Attacks on connected physical systems can be considered in three dimensions:

- the type of person attacking the system (e.g. a person from inside or outside the organization);
- the attacker's goals and tasks (e.g. destruction of a specific target or on a larger scale);
- attack mode (e.g. active or passive) (Khalid et al., 2018).

Moreover, in the literature on the subject you can find information about three main layers in which cybersecurity threats may operate:

- conscious action layer (e.g. sensors and actuators);
- data transport layer (e.g. from the network architecture);
- application control layer (e.g. from storing user data).

The first layer includes physical attacks, equipment failures, electromagnetic interference, and power line node failures. In the second layer, there are denial of service attacks, attacks on aggregation nodes, flood attacks (exhaustion of network resources), routing attacks, black holes, misdirection attacks, and Sybil attacks by adding malicious nodes. In turn, the third layer is characterized by unauthorized access, control of machines, sending malicious code, and leaking private user and confidential data during data mining operations (Roy et al., 2016).

The German Federal Office for Information Security (Bundesamt för Sicherheit in der Informationstechnik – BSI) has identified the following categories of cyber threats relating to the Industry 4.0 context:

- direct attacks on external access;
- indirect attacks on the IT systems of a service provider that has been granted external access;
- unknown attack vectors with no ability to detect through unknown vulnerabilities;
- untargeted malware that infects components and impairs their functionality;

- intrusion into neighbouring networks or network segments (Flatt et al. 2016).

Smart manufacturing depends heavily on data-driven innovation to ensure seamless integration of cyber and physical spaces. Easy access to commercial IoT platforms such as GE Predix, IBM Watson or Microsoft Azure enables communication and integration between physical "things" and applications in cyberspace. However, IoT is still in the development phase and encounters technical problems related to cyberphysical integration in the production system, i.e. communication, Big Data, control and protection (Yang et al., 2019).

In the early 1980s, common cyber-attacks involved password cracking and password guessing. Currently, targeted cyber-attacks include advanced scanning, keyloggers and denial-of-service attacks. Cyber-attacks are expected to become more sophisticated in the future, seeking out and damaging strategic points using bots, malicious codes and morphing (Ervural & Ervural, 2018).

To successfully implement effective Industrial IoT security, specific rules must be followed to ensure the security of the entire Industrial IoT system (Luiijf et al., 2011):

- *Confidentiality* is a key element of industrial IoT security, but in certain situations where data is published, this may not be necessary. It protects information from unauthorized access using encryption and access restriction algorithms, which is important for data such as patient information, business and military data, and credentials and secret keys (Fink et al., 2017).
- *Integrity* is a mandatory security feature in IoT systems, ensuring reliable services and protecting data from unauthorized manipulation, both external and internal. Different IoT systems have different requirements for integrity, and the lack of it can lead to serious consequences, such as erroneous data in remote patient monitoring, which in extreme cases can result in death (Thames & Schaefer, 2017).
- *Authentication* of ubiquitous IoT connectivity relies on the industrial nature of the environment where Machine2Machine, human-to-device and/or human-to-human communication is possible. Different authentication requirements necessitate different system solutions. For example, bank cards or banking systems may require strong authentication to ensure access is restricted to authorized entities. Additionally, some systems need to be designed for international use, while others are intended for local use (Khalid et al., 2020).
- *Privacy* is the right of an individual to decide whether and to what extent he or she shares information about himself or herself with others. In the context of the Industrial Internet of Things (IIoT), the main privacy objectives include:
    - *Device Privacy:* Includes physical protection and switching security. The idea is to prevent the disclosure of confidential information in the event of theft, loss or side-channel attacks.
    - *Storage Privacy:* Refers to the protection of data stored on devices. The key aspects are minimizing the amount of stored data and securing data after the end of the device's life, especially in the event of its theft, loss, or disuse.
    - *Privacy of communications:* Depends on the availability, integrity, and reliability of the device. IoT devices should only communicate when necessary to protect user data.
    - *Privacy of processing:* Covers the protection of data against disclosure or retention by third parties without the knowledge of the data owner.
    - *Privacy Identity:* Device identity should only be identified by an authorized person or device.
    - *o Privacy Location:* Only an approved entity should have access to the geographic location of the device (Khalid et al., 2020).

Foundations of Industry 4.0 in the European Union

EU economies are being transformed by new production models driven by technological change, including the diffusion of digital technology, new business models and forms of demand. Advanced technologies are the basis of the 'fourth industrial revolution' that has the potential to transform the EU industry and deliver economic growth. Most EU governments are making Industry 4.0 a priority, introducing policies on a national scale to increase productivity and competitiveness and developing advanced skills for workers. Although there is a large overlap between Member States' policy objectives and strategies, there is a lack of systematic cooperation and exchange of good practices (Erasmus+ I4EU, 2022).

Industry 4.0 in the EU economy aims to transform the entire industrial ecosystem, making it faster, autonomous and customer-centric, contributing to new business opportunities. Here are some aspects of the industrial revolution:

1. *Business models:* The use of data enables new services and production optimization, especially in industries such as the semiconductor industry.
2. *Value networks:* Collaboration between producers enables the exchange of resources and information, leading to new business models.
3. *Customization:* Customer-centric production allows you to meet needs faster through flexible production systems.
4. *Equipment:* Automated tools and cooperation between workers and machines increase the efficiency of production processes.
5. *Workers:* Automation can reduce the number of workers while requiring new skills.
6. *Product and process:* The development of technology leads to a decrease in production costs and an improvement in product quality thanks to the use of real-time data.

These changes can result in increased productivity and efficiency, supported by advanced analytics and predictive maintenance (Erasmus+ Footin 4.0, 2020).

European industries exhibit varying degrees of adoption and investment in Industry 4.0 (I40) technologies. Manufacturing leads in investment due to its focus on production processes, while logistics increasingly relies on data analysis for inventory and route optimization, driven by the growth of e-commerce. Utilities benefit from Big Data Analytics (BDA) for improved resource allocation and production efficiency. In contrast, industries like construction lag in all dimensions of Industry 4.0 adoption, indicating a failure to fully harness its benefits. Hospitality, despite having a strong infrastructure base, demonstrates low implementation levels in Big Data Maturity (Castelo-Branco et al., 2023).

At the national level, European Union member states vary in their approaches to implementing Industry 4.0. Some countries, such as Bulgaria, the Czech Republic, Greece, Hungary, Latvia, Poland, Romania, and Slovakia, have more than 50% falling below the average. Conversely, Denmark, Finland, the Netherlands, and Sweden stand out for their effective adaptation to the Fourth Industrial Revolution, having invested not only in Industry 4.0 infrastructure but also in its practical applications. Regarding Big Data Maturity, Finland and the Netherlands are leading the pack, joined by France and Luxembourg. Across the EU28, a higher percentage falls below the average (33%), with Infrastructure Focused and Big Data Leaders comprising 22% of the total (Castelo-Branco et al., 2023).

Advanced technologies are driving the fourth industrial revolution, poised to revolutionize EU industries and catalyze significant growth in the European economy. Rather than birthing new sectors, Europe's digital

potential lies in the metamorphosis of existing industries and enterprises, as highlighted by the Digital Transformation Monitor 2017 (EU, 2017). Despite challenges evidenced by the low adoption rates of digital technologies among EU enterprises, there's optimism: 75% of surveyed EU businesses view digital technologies as an opportunity, with 64% reporting positive outcomes from their investments (EU, 2017). Policy recommendations (Interreg Europe Policy Learning Platform 2019. Launched in March 2017 is at the core of the coordination effort of the European Commission. The Platform plays an essential role in the roll-out of digitalisation of industry across Europe by supporting experience exchange, and collaboration, triggering joint investments, common approaches to regulatory frameworks, and measures for staff up- and re-skilling), which can have a positive impact on the European economic development in the field of Industry 4.0 are:

- *Devise Regional Industry 4.0 Strategies*. Regions with significant industrial bases should develop Industry 4.0 strategies, requiring policymakers to collaborate closely with the private sector for effective implementation. This recommendation is particularly pertinent for regions with industrial bases exceeding 18% of regional GDP.
- *Support the Creation of Makerspaces in Higher Education Institutions*. The second recommendation urges regions to promote the use of maker spaces in higher education institutions. Makerspaces, defined as community centres offering technology and manufacturing tools, provide valuable skills aligned with industry 4.0 demands, thus preparing students effectively.
- *Adopt Responsible Criteria in Public Procurement Tenders*. The third policy recommendation suggests that regions should implement responsible criteria in public tenders. Emerging technologies like Big Data, AI, and cybersecurity, used in Industry 4.0, raise significant ethical considerations.
- *Promote Public-Private Partnerships to Diffuse Industry 4.0 Technological Innovations*. The fourth recommendation suggests regions should encourage public-private partnerships (PPP) to spread Industry 4.0 innovations, particularly to small and medium enterprises (SMEs). The Swift and effective diffusion of these technologies is crucial for economic progress. International technology diffusion influences productivity and growth, with a few wealthy nations driving most of the new technology creation.
- *Promote Diffusion of Industry 4.0 Technological Innovations in Lagging Regions.* The fifth policy recommendation underscores the importance for underdeveloped areas to encourage the spread of Industry 4.0 technologies. In these regions, policymakers often overestimate their innovation capabilities, necessitating policies that facilitate technology diffusion. Strategies should focus on enhancing the capacity of local stakeholders, particularly SMEs, to adopt and adapt these innovations to the regional context.
- *Promote Disruptive Industry 4.0 Technological Innovations in Leading Innovative Regions.* The sixth policy recommendation advises leading innovative regions to promote disruptive Industry 4.0 technologies. Regions identified as innovation leaders should drive the next wave of radical innovations to maintain their technological edge and leadership (Erasmus+ I4EU, 2022).

Table 1 presents the European Union Member States have already launched national initiatives for the digitisation of industry

Table 1: EU national initiatives for the digitisation of industry

Country	Initiatives
Austria	• Industrie 4.0 Österreich (https://plattformindustrie40.at/?lang=en) • Digital Roadmap Austria (https://www.digitalroadmap.gv.at/)

Belgium	• MADE DIFFERENT – Factories of the future (http://www.madedifferent.be/) • Flemish initiative on Industrie 4.0 (https://www.vlaanderen.be/nl/publicaties/detail/vision-2050) • Digital Wallonia (https://www.digitalwallonia.be/madedifferent-digital-wallonia/)
Bulgaria	• No information
Croatia	• Digitising Impulse 2020
Country	**Initiatives**
Cyprus	• National Integrated Industrial Strategy 2017 – 2030
Czech Republic	• Průmysl 4.0 (https://www.mpo.cz/en/industry/industry-four/)
Denmark	• MADE - Manufacturing Academy of Denmark (http://made.dk/)
Estonia	• No information
Finland	• Digitising the Finnish Industry program
France	• Alliance Industrie du Futur (http://www.industrie-dufutur.org) • Programme des Investissements d'Avenir (http://www.gouvernement.fr/investissements-d-avenir-cgi) • Transition Numerique (www.transition-numerique.fr)
Germany	• Plattform Industrie 4.0 (www.plattform-i40.de) • Mittelstand 4.0 (http://www.mittelstanddigital.de/DE/Foerderinitiativen/mittelstand-4-0.html)
Greece	• No information
Hungary	• IPAR4.0 Technology Platform (https://www.i40platform.hu)
Ireland	• No information
Italy	• Piano Nazionale Industria 4.0 (http://www.mise.gov.it/index.php/it/industria40)
Latvia	• No information
Lithuania	• Pramonė 4.0 (http://www.industrie40.lt/platform/)
Luxembourg	• Digital4Industry - D4I (http://digital4industry.lu/)
Malta	• No information
Netherlands	• Smart Industry - Dutch Industry Fit for the Future (http://www.smartindustry.nl)
Poland	• Platforma Przemysłu Przyszłosci – PPP (https://przemyslprzyszlosci.gov.pl/)
Portugal	• Indústria 4.0 (www.i40.pt)
Romania	• No information
Slovakia	• Conception of Smart Industry for Slovakia
Slovenia	• No information
Spain	• Industria Conectada 4.0 (http://www.industriaconectada40.gob.es)
Sweden	• No information

(**Kulykovets, 2024)**

In 2021, only 55% of small and medium-sized enterprises (SMEs) reached at least a basic level in the adoption of digital technologies. Sweden and Finland have the most digitalised SMEs (86% and 82% having a basic level of digital intensity respectively), while Romania and Bulgaria have the lowest rates of SME digitalisation. To reach the Digital Decade target, at least 90% of SMEs in the EU should have a basic level of digital intensity by 2030 (EU, 2022a).

Businesses are getting more and more digitalised, but the use of advanced digital technologies remains low. Although already 34% of enterprises rely on cloud computing (in 2021), only 8% use AI (in 2021) and 14% Big Data (in 2020). Following the Path to the Digital Decade proposal, at least 75% of companies should take up AI, cloud, and Big Data technologies by 2030 (EU, 2022a).

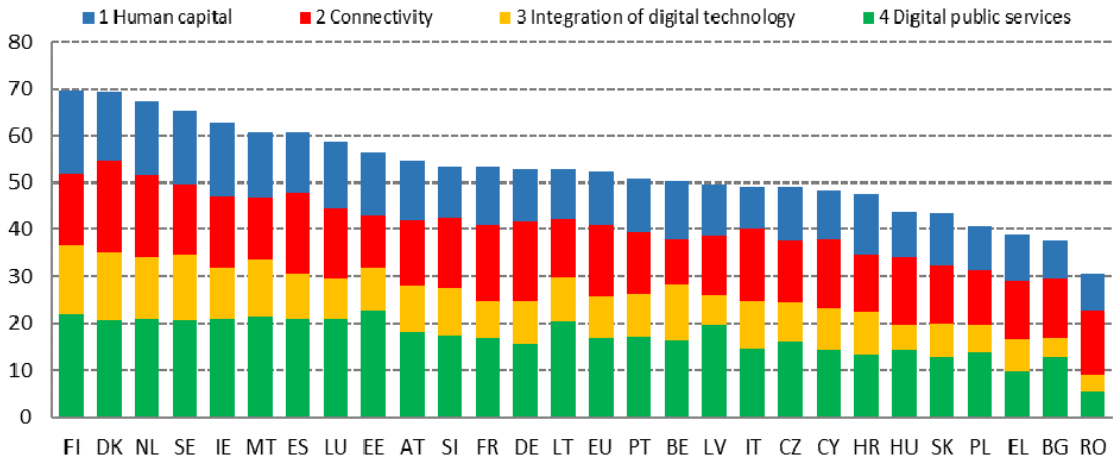

Figure 1: Digital Economy and Society Index, 2022 (Source: DESI 2022, European Commission)

There is a substantial gap between large companies and SMEs, not only in the use of advanced technologies but also in basic digital solutions, such as having an enterprise resource planning (ERP) software package and engaging in e-commerce. Finland, Denmark and Sweden rank highest overall in the digital transformation of businesses. Figure 1 shows the Digital Economy and Society Index (2022). The most advanced digital economies in the EU are Finland, Denmark, the Netherlands, Sweden, Ireland, Malta and Spain. The lowest DESI scores are in Romania, Bulgaria, and Greece.

Digital technologies provide businesses with competitive advantages, enhance services and products, and help expand markets. A McKinsey study found that 93% of EU executives see better data access as crucial, with 40% considering it very important (EU, 2022b). OECD (2015) research indicates that companies investing in data-driven innovation and analytics grow 5-10% faster than those that don't. The EU's digital sovereignty relies on the ability to store, extract, and process data securely, requiring advanced infrastructure and technologies. This includes developing energy-efficient, climate-neutral services and reducing dependency on imports, especially semiconductors. The DESI dimension evaluates business digitalization and e-commerce, focusing on technologies like Big Data analytics, cloud services, and AI, as well as the prevalence of e-commerce among SMEs. It also measures ICT's role in environmental sustainability efforts within enterprises (EU, 2022a).

Large corporations tend to embrace new technologies more readily. For instance, electronic information sharing via enterprise resource planning (ERP) software is significantly more prevalent in large corporations (81%) than in small and medium-sized enterprises (SMEs) (37%). On social media, over twice as many large corporations (61%) utilize these platforms compared to SMEs (28%). SMEs take advantage of e-commerce opportunities to a lesser degree, with just 18% engaging in online sales (versus 38% of large corporations) and only 9% conducting cross-border online sales (versus 24% of large corporations). Numerous other technological advancements, such as cloud services, AI, and Big Data, remain underutilized by SMEs (Figure 2) (EU, 2022a).

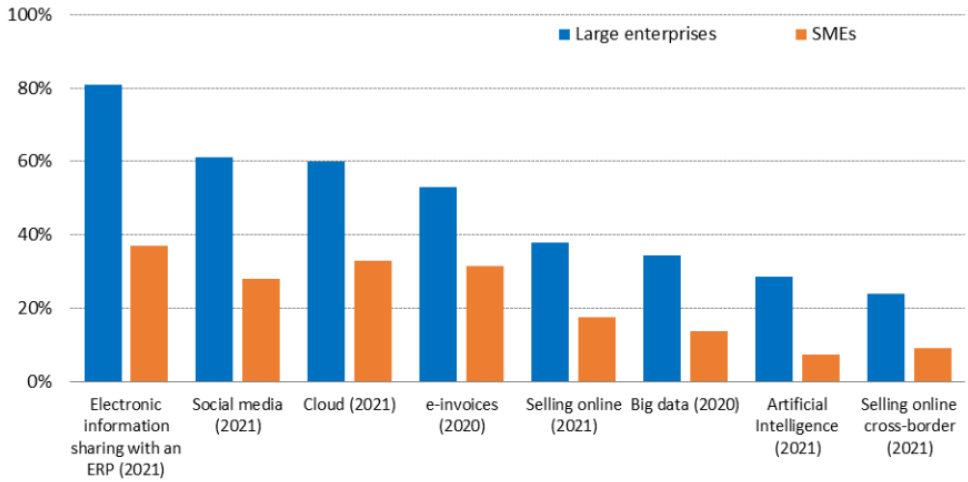

Figure 2: Adoption of digital technologies (% enterprises), 2020, 2021(Source: Eurostat, European Union survey on ICT usage and e-commerce in enterprises.)

In its Path to the Digital Decade proposal, the European Commission aims for the following targets by 2030 in digital technology integration: over 90% of European SMEs achieving basic digital intensity, 75% of EU companies using cloud, AI, and Big Data, and doubling the number of EU unicorns through enhanced scale-ups and financing. A unicorn is a privately held start-up company valued at over USD 1 billion. This is a stage of the start-up financial development which proves its maturity and success on the global market. In order to be considered a unicorn, a company has to steadily and dynamically grow through all the development phases supported by the start-up ecosystem.According to Dealroom, as of March 2022, there were 2,282 unicorns in the world. The EU has only 222 (an increase from 143 in summer 2021) unicorns, as opposed to 1 243 (an increase from 889) in the US, 530 (an increase from 414) in Asia (out of which 306 (an increase from 272) in China) and 119 (an increase from 101) in the UK (Dealroom, 2024).

Table 2: Most valuable unicorns in the EU 2022 (Dealroom.co 2024)

Name	*Location*	*Type*	*Market*	*Valuation (billion USD)*
Adyen	Amsterdam Netherlands	Machine learning Artificial intelligence Commission Saas	B2B Fintech Payments	56.8
Spotify	Stockholm Sweden	Machine learning Artificial intelligence Subscription	B2C Music Media Streaming	52.0
Klarna	Stockholm Sweden	Commission	B2B, B2C Fintech Payments	45.6
BioNTech	Mainz Germany	Machine learning Artificial intelligence Deep tech	B2B Health Biotechnology	36.4
Flutter Entertainment	Dublin Ireland	Commission	B2C Gaming Betting & Gambling	29.4

Name	Location	Type	Market	Valuation (billion USD)
Genmab	Copenhagen Denmark	Deep tech Machine learning Artificial intelligence	B2B Health Biotechnology	17.4
Delivery Hero	Berlin Germany	Commission Marketplace & Commerce	B2C Food Food Logistics and delivery	15.2
Zalando	Berlin Germany	Artificial intelligence Marketplace & Commerce	B2C Fashion Footwear	13.7
ARGEN-X	Ghent Belgium	Commission	B2B Health Biotechnology	13.0
Oatly	Malmo Sweden	Selling own inventory Manufacturing	B2C Food Innovative food	13.0
AUTO1 Group	Berlin Germany	Marketplace & Commerce	B2C Transportation Search, buy & rent	12.9
CureVac	Tubingen Germany	Manufacturing	B2B Health Biotechnology	12.8

In the EU, out of the 12 most valuable EU unicorns, five are located in Germany, three in Sweden and the Netherlands, Ireland, Denmark and Belgium each have one (Table 2) (EU, 2022a). Key elements significantly contribute to facilitating and enhancing the adoption of cloud services, Big Data, and AI. One such element is having a workforce with advanced digital skills. Moreover, providing legal clarity and tackling issues related to data protection and liability is crucial for enabling data usage and minimizing the risks associated with security breaches and data protection violations (EU, 2022a).

Discussion

Industry 4.0, together with related technologies such as cloud-based design, manufacturing systems and the Internet of Things, offers new opportunities to create value in major market sectors through disruptive innovations. However, cybersecurity and data privacy issues pose significant challenges that may prevent Industry 4.0 from fully realizing its potential (Thames & Schaefer, 2017). In today's rapidly evolving environment, cybersecurity is anticipated to become a crucial element in the strategy, design, and operations of companies adopting the Industry 4.0 framework (Lezzi et al., 2018).

The impact of Industry 4.0 is also visible in other service industries (Castelo-Branco et al., 2023). Tourism can leverage advanced automation technologies such as artificial intelligence, robotics, and the Internet of Things (IoT), which are the foundation of the idea of intelligent tourism ecosystems (Tussyadiah, 2020). In utilities, interconnection and autonomous data exchange between producers and consumers enable the development of smart grid systems with optimized controls and the ability to manage available power most efficiently (Faheem et al., 2018). Information and communications, including publishing,

telecommunications, data processing and storage, is a leader in the use of connected Industry 4.0 technologies. Companies rely primarily on wireless communications and cloud computing to streamline internal operations and expand services to customers (Castelo-Branco et al., 2023).

From the EU's standpoint, Industry 4.0 could serve as both a defensive measure (by helping to sustain its manufacturing sector) and a proactive strategy (by boosting productivity and opening up new market opportunities) (Teixeira & Tavares-Lehmann, 2022). A key funding source for Industry 4.0 projects is EU programs. Supporting these projects is a major priority in EU development policy, to promote the adoption of Industry 4.0 across the region (Wyrwa, 2020). Enhancing innovation activities within the EU is becoming a crucial strategy for revitalizing the European economy and boosting Europe's global competitiveness. This introduces new challenges for the EU's industrial policy for 2021-2027, particularly regarding its goals, instruments, and mechanisms for research, technological development, and innovation (EU, 2019).

References

Arnold, C., Kiel, D., Voigt, K. (2016). How the Industrial Internet of Things changes business models in different manufacturing industries. *International Journal of Innovation Management*, vol. 20 (8). https://doi.org/10.1142/S1363919616400156

Barreto, L., Amaral, A., Pereira, T. (2017). Industry 4.0 implications in logistics: An overview. *Procedia Manufacturing*, 13, 1245–1252. https://doi.org/10.1016/j. promfg.2017.09.045

Bauer, H., Scherf, G., von der Tann, V. (2017, August 31). *Six Ways CEOs Can Promote Cybersecurity in the IoT Age.* McKinsey & Company. https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age

Ben-Daya, M., Hassini, E., Bahroun, Z. (2019). Internet of Things and supply chain management: A literature review. *International Journal of Production Research*, 57 (15–16), 4719–4742. https://doi.org/10.1080/00207543.2017.1402140

Castelo-Branco, I., Amaro-Henriques, M., Cruz-Jesus, F., Oliveira, T. (2023). Assessing the Industry 4.0 European divide through the country/industry dichotomy. *Computers & Industrial Engineering*, vol. 176, 1-14. https://doi.org/10.1016/j.cie.2022.108925

Cisco. (2018, February). *Annual Cybersecurity Report*. https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Culot, G., Nassimbeni, G., Orzes, G., Sartor, M. (2020a). Behind the definition of Industry 4.0: Analysis and open questions. *International Journal of Production Economics*, 226 (3), 55. https://doi.org/10.1016/j.ijpe.2020.107617

Culot, G., Orzes, G., Sartor, M., Nassimbeni, G. (2020b). The future of manufacturing: A Delphi-based scenario analysis on Industry 4.0. *Technological Forecasting and Social Change*, 157, 120092. https://doi.org/10.1016/j.techfore.2020.120092

Dealroom.co. Global provider of data and intelligence on startups and tech ecosystems. Access: 7.05.2024. https://dealroom.co/reports

Erasmus+ Footin 4.0. (2020). *Study on Industry 4.0 applied to the footwear industry in Europe*. https://ec.europa.eu/programmes/erasmus-plus/project-result-content/704e8b0f-ae33-49e9-9dfa-e2601e7e4fba/O1_Study_about_I4.0_PL.pdf

Erasmus+ I4EU. (2022). *I4EU Handbook*. Project Key competences for an European model of Industry 4.0 (Project Index Number 2019-1-FR01-KA202-062965). https://www.i4eu-pro.eu/wp-content/uploads/sites/2/2022/07/Key-competences-for-an-European-model-of-Industry-4.0-Version-4_compressed.pdf

Ervural, B.C., Ervural, B. (2018). Overview of Cyber Security in the Industry 4.0 Era. In A. Ustundag, E. Cevikcan (Ed.), *Industry 4.0: Managing The Digital Transformation. Springer Series in Advanced Manufacturing* (pp. 267-284). Springer. https://doi.org/10.1007/978-3-319-57870-5_16

European Commission (2019). *Proposal for a Decision of the European Parliament and of the Council on the Strategic Innovation Agenda of the European Institute of Innovation and Technology (EIT) 2021-2027: Boosting the Innovation Talent and Capacity of Europe*. https://ec.europa.eu/education/sites/education/files/document-library-docs/proposal-decision-eit-2021-2027.pdf.

European Commission. (2017, May). *Digital Transformation Monitor (DTM). Key lessons from national Industry 4.0 policy initiatives in Europe*. https://es.sistematica.it/docs/379/DTM_Policy_initiative_comparison_v1.pdf

European Commission. (2022a, August). *Digital Economy and Society Index (DESI) 2022*. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022

European Commission. (2022b, September). *Shaping the digital transformation in Europe*. [McKinsey & Company]. https://digital-strategy.ec.europa.eu/en/library/shaping-digital-transformation-europe

European Cyber Security Organisation (ECSO). (2017, December). *State of the Art Syllabus – Overview of Existing Cybersecurity Standards and Certification Schemes*. https://www.ecs-org.eu/documents/publications/5a31129ea8e97.pdf

European Monitor of Industrial Ecosystems (EMI). (n.d.). *Industrial Ecosystems*. Access 12.05.2024 https://monitor-industrial-ecosystems.ec.europa.eu/

European Union Agency for Networked and Information Security (ENISA). (2018, November). *Good Practice for Security of Internet of Things in the Context of Smart Manufacturing*. https://op.europa.eu/en/publication-detail/-/publication/96180e8b-0340-11e9-adde-01aa75ed71a1/language-en

Faheem, M., Shah, S. B. H., Butt, R. A., Raza, B., Anwar, M., Ashraf, M. W., Gungor, V. C. (2018). Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Computer Science Review*, 30, 1 – 30. https://doi.org/10.1016/j.cosrev.2018.08.001

Fernandez-Carames, T. M., Fraga-Lamas, P. (2018). A review on human-centered IoT- connected smart labels for the Industry 4.0. *IEEE Access*, 6, 25939 – 25957. https:// doi.org/10.1109/ACCESS.2018.2833501

Fink, G. A., Edgar, T. W., Rice, T. R., MacDonald, D. G., Crawford, C. E. (2017). Overview of Security and Privacy in Cyber-Physical Systems. In H. Song, G. A. Fink, S. Jeschke (Ed.), *Security and Privacy in Cyber-Physical Systems. Foundations, Principles and Applications* (pp. 1-48). Wiley.

Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., Adamczyk, H. (2016). *Analysis of the cyber-security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements*. EEE International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany.

Fortune Business Insights. Smart Manufacturing Market. (Update May 6, 2024). https://www.fortunebusinessinsights.com/smart-manufacturing-market-103594#

Frost & Sullivan White Paper. (2017). *Cyber Security in the Era of Industrial IoT*. https://www.frost.com/files/5314/8941/8579/CYBER_SECURITY_IN_THE_ERA_OF_INDUSTRIAL_IOT.pdf

Gubán, M., Kovács, G. (2017). Industry 4.0 Conception. *Acta Technica Corviniensis - Bulletin of Engineering*, t. X, 111 – 115. https://www.proquest.com/scholarly-journals/industry-4-0-conception/docview/1869485942/se-2

Hofmann, E., Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, 89, 23–34. https://doi.org/10.1016/j.compind.2017.04.002

International Electronical Commission (IEC). (2018, June). *IEC GUIDE 120:2018. Security aspects - Guidelines for their inclusion in publications*. https://webstore.iec.ch/publication/62122

Khalid, A., Kirisci, P. T., Khan Z. H., Ghrairi Z., Thoben, K.-D., Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, vol. 97, 132-145. 10.1016/j.compind.2018.02.009

Khalid, H., Hashim, S.J., Ahmad S. M. S., Hashim, F., Chaudary, M. A. (2020). Cybersecurity in Industry 4.0 context: background, issues, and future directions. In W. Y. Leong, J. H. Chuah, B. T. Tee (Ed.), *The Nine Pillars of Technologies for Industry 4.0* (pp. 263-307). The Institution of Engineering and Technology.

Kusiak, A. (2017). Smart manufacturing. *International Journal of Production Research*, vol. 56 (1-2), 508-517. https://doi.org/10.1080/00207543.2017.1351644

Lasi, H., Fettke, P., Kemper, H. G., Feld, T., Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, 6, 239–242. https://doi.org/10.1007/s12599-014-0334-4

Lezzi, M., Lazoi, M., Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, vol. 103, 97-110. https://doi.org/10.1016/j.compind.2018.09.004

Lu, Y., Xu, X., Wang, L. (2020). Smart manufacturing process and system automation – A critical review of the standards and envisioned scenarios. *Journal of Manufacturing Systems*, vol. 56, 312-325. https://doi.org/10.1016/j.jmsy.2020.06.010

Luiijf, E., Besseling, K., Spoelstra, M., de Graaf, P. (2011, September 8-9). *Ten National Cyber Security Strategies: a Comparison.* Critical Information Infrastructure Security. 6th International Workshop on Critical Information Infrastructures Security. Lucerne, Switzerland.

Manyika, J. (2017). *A future that works: AI automation employment and productivity.* McKinsey Global Institute. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/170622-slides-manyika.pdf

Moghaddam, M., Cadavid, M.N., Kenley, C.R., Deshmukh, A.V. (2018). Reference architectures for smart manufacturing: A critical review. *Journal of Manufacturing Systems*, vol. 49, 215-225. https://doi.org/10.1016/j.jmsy.2018.10.006

Munirathinam, S. (2020). Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT). *Advances in Computers*, vol. 117 (1), 129-164. https://doi.org/10.1016/bs.adcom.2019.10.010

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. (2013, May) *Glossary of Key Information Security Terms*. https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

OECD. (2015). *Data-driven Innovation: Big Data for Growth and Well-Being*. [OECD Publishing]. https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm

Phuyal, S., Bista, D., Bista, R. (2020). Challenges, Opportunities and Future Directions of Smart Manufacturing: A State of Art Review. *Sustainable Futures*, vol. 2, 100023. https://doi.org/10.1016/j.sftr.2020.100023

Roy, R., Stark, R., Tracht, K., Takata, S., Mori, M. (2016). Continuous maintenance and the future – foundations and technological challenges. *CIRP Annals*, vol. 65 (2), 667-688. https://doi.org/10.1016/j.cirp.2016.06.006

Sahoo, S., Lo, C.-Y. (2022). Smart manufacturing powered by recent technological advancements: A review. *Journal of Manufacturing Systems*, vol. 64, 236-250. https://doi.org/10.1016/j.jmsy.2022.06.008

Teixeira J. E., Tavares-Lehmann A. T. C. P. (2022). Industry 4.0 in the European Union: Policies and national strategies. *Technological Forecasting and Social Change*, vol. 180, 121664. https://doi.org/10.1016/j.techfore.2022.121664

Thames, L., Schaefer, D. (2017). Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges. In L.Thames, D. Schaefer (Ed.), *Cybersecurity for Industry 4.0. Springer Series in Advanced Manufacturing Analysis for Design and Manufacturing (pp. 1-33)*. Springer.

Tussyadiah, I. (2020). A review of research into automation in tourism: Launching the Annals of Tourism Research Curated Collection on Artificial Intelligence and Robotics in Tourism. *Annals of Tourism Research*, vol. 81, 102883. https://doi.org/10.1016/j.annals.2020.102883

Weber, K. M., Schaper-Rinkel, P. (2017). European sectoral innovation foresight: Identifying emerging cross-sectoral patterns and policy issues. *Technological Forecasting and Social Change*, 115 (C), 240–250. https://doi.org/10.1016/j. techfore.2016.09.007

Wyrwa, J. (2020). A review of the European Union financial instruments supporting the innovative activity of enterprises in the context of Industry 4.0 in the years 2021-2027. *Entrepreneurship And Sustainability Issues*, vol. 8 (1), 1146-1161. ttps://doi.org/10.9770/jesi.2020.8.1(77)

Yang, H., Kumara, S., Bukkapatnam, S.T.S., Tsung F. (2019). The Internet of Things for smart manufacturing: A review. *IISE Transactions*, vol. 51 (11), 1190-1216. https://doi.org/10.1080/24725854.2018.1555383

Zhang, C., Yang, J. (2020). *A History of Mechanical Engineering*. Springer. https://doi.org/10.1007/978-981-15-0833-2_1