

Review

From Industry 4.0 to Industry 5.0 in the Field of Autonomous Robots: Expectations, Telecommunications Operator Opportunities, and Security Challenges

Tomasz W. Nowak ¹, Mariusz Sepczuk ¹, Zbigniew Kotulski ^{1,*}, Tomasz Pawlikowski ², Aleksandra Podlasek ², Krzysztof Bocianiak ² and Jean-Philippe Wary ³

¹ Faculty of Electronics and Information Technology, Warsaw University of Technology, 00-665 Warsaw, Poland; tomasz.nowak@tnowak.pl (T.W.N.); mariusz.sepczuk@pw.edu.pl (M.S.)

² Orange Polska S.A., 02-326 Warsaw, Poland; tomasz.pawlikowski@orange.com (T.P.); aleksandra.podlasek@orange.com (A.P.); krzysztof.bocianiak@orange.com (K.B.)

³ Orange Innovation, 92320 Châtillon, France; jeanphilippe.wary@orange.com

* Correspondence: zbigniew.kotulski@pw.edu.pl

Abstract

Industry 4.0, expected to limit the burden of manual labor through the integration of cyber-physical systems, the Internet of Things (IoT), and machine learning methods, failed to meet social expectations. It started excluding humans from the production process. The next stage of the industrial revolution, Industry 5.0, reverses this trend by emphasizing the importance of human involvement and interaction in production processes. In this paper, we present the evolution of robotic systems, from those of Industry 4.0 to their humanized versions expected in Industry 5.0, with a particular emphasis on system cybersecurity. Moreover, we present the challenges and business opportunities that telecommunications operators face in implementing and operating robotic cyber-physical systems. We also analyze new security challenges arising from this transformation and the central role of humans in industrial processes. We illustrate the identified problems with a special case: Cobots.

Keywords: Cobots; cognitive systems; digital twins; human-centric technologies; Industry 5.0

1. Introduction

The development of manufacturing methods, initiated by improving materials and handicraft tools, accelerated dramatically when humans came up with the idea of supplementing the physical strength of people and animals with external energy sources. The current course of development of industrial technologies can be presented as a five-step transformation, known as the Industrial Revolution [1]. The first industrial revolution, which started at the end of the eighteenth century, involved harnessing the power of water and steam, freeing people from the most strenuous, monotonous physical labor. Industry 2.0 (initiated by the Second Industrial Revolution in the nineteenth century) used electricity to intensify production by building assembly lines and mass-production systems. The third revolution and Industry 3.0 (the second half of the twentieth century) sought to support employees' intellectual work through the use of computers and electronic systems, as well as through automation. Industry 4.0, which began in the twenty-first century, has led to the integration of production processes with telecommunications systems through



Academic Editor: Giuseppe Prencipe

Received: 17 April 2026

Revised: 26 June 2026

Accepted: 2 July 2026

Published: 8 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

the use of cyber-physical systems, networking, and the IoT, particularly Industrial IoT (IIoT). It has also moved further toward intervening in human roles in the production process, reducing routine manual and administrative tasks. The use of machine learning systems could ultimately lead to the elimination of humans from increasingly advanced management and supervisory roles. On the other hand, new technologies require employees with advanced competencies, who are constantly upskilling and taking on new roles: robotics engineers, cybersecurity specialists, Big Data analysts, and systems architects [2]. Despite its promising technological potential, it is argued that Industry 4.0 has not fully met societal expectations [3–5]. Its implementation remains mainly focused on technology and productivity rather than on people, whilst technological evolution concentrates more on systems and machines than on people. This approach is associated with negative socio-environmental consequences, such as exclusion from the labor market, economic inequalities, the digital divide, and business instability. More broadly, it has been noted that Industry 4.0, as a technology-driven phenomenon, has systematically overlooked many aspects of socio-environmental sustainability. It is precisely this discrepancy between technological capabilities and people-centered outcomes that has motivated the emergence of the Industry 5.0 paradigm, which places the well-being of industrial workers at the heart of the production process, moving beyond mere job creation towards a resilient model of shared prosperity. However, it should be noted that Industry 4.0 can also have positive effects, particularly on workplace safety and productivity, including a safer working environment, improved staff health, and a reduction in occupational risks [6,7]. These benefits are generally regarded as partial and unevenly distributed across different sectors, and Industry 5.0 aims to extend and consolidate them.

Industry 5.0 [8–10] is a term used to describe the next phase of the industrial revolution, focusing on the relationship between humans and machines within the manufacturing industry. It is a concept based on Industry 4.0 advances, emphasizing the integration of robotic systems, the Internet of Things (IoT), and Big Data analytics to improve manufacturing processes. However, Industry 5.0 emphasizes the importance of human involvement and interaction across industries. The concept of Industry 4.0 has brought significant improvements in manufacturing efficiency. Still, it has also raised concerns about the impact of automation on labor and the loss of human involvement in the manufacturing process. Industry 5.0 addresses these concerns by emphasizing human–machine collaboration and developing more natural, intuitive methods for human–machine interaction. Thus, Industry 5.0 presents the opportunity to create a more sustainable and humane manufacturing industry. By emphasizing the human element in manufacturing, Industry 5.0 can help create more fulfilling and rewarding jobs for workers and improve working conditions. It also offers the potential to develop more efficient and flexible manufacturing processes, better equipped to adapt to changing market demands and supply chain disruptions.

The main achievement of Industry 4.0 in relieving workers was automation and robotization through the deep integration of digital technologies (like Artificial Intelligence, Internet of Things, and cyber-physical systems) into physical production. Industry 5.0 does not intend to abandon this achievement, but it strives to adapt it to new societal expectations, shifting the industrial paradigm from pure technological automation to human–machine collaboration. Society now expects industries to prioritize well-being, sustainability, and resilience alongside economic growth [11,12]. In this paper, we present the new challenges associated with adapting robotic solutions and fundamental technologies used in Industry 4.0 to the expectations of Industry 5.0. We present differences in the use of autonomous robots across the two most recent industrial generations, as well as the expectations placed on collaborative robots in Industry 5.0. We also analyze the challenges emerging in the robotic environment, particularly those related to the new tasks

telecommunications operators face. In particular, this concerns new operators' opportunities and challenges in providing Information Technology (IT) resources for secure and reliable communication and customer support. We present new system security threats resulting from the changing relationship between human and technological factors. We also examine the challenges faced by different parties in migrating autonomous robot applications from Industry 4.0 to Industry 5.0. The main contributions of this study are as follows:

- We have described how the technologies used in Industry 4.0 and Industry 5.0 are evolving, and we have also outlined the evolution of pillar technologies in robotics: from Industry 4.0 to Industry 5.0.
- We have demonstrated scenarios in which Cobots can be used in Industry 5.0 and proposed a new architecture for Cobot-based use cases, which was analyzed in the context of the CAP theorem [13] and fundamental challenges of distributed architectures.
- We have outlined how a telecommunications operator can get involved in Cobot scenarios. This original synthesis was developed from the perspective of Industry 5.0 pillars and various network service offerings.
- We have listed the safety challenges and risks associated with Cobots in Industry 5.0. We have conducted an original comparison of their significance in the context of Industry 4.0 and Industry 5.0, respectively.

This article addresses only selected issues relating to the use of Cobots in Industry 5.0. Aspects such as ethics, privacy, personal data protection, medical data, general compliance, and accountability have not been discussed, as this article serves as an introduction to more detailed topics that are, however, essential for the proper functioning of the service in question. Those aspects might be important for practical implementations of the presented ideas.

The rest of the paper is as follows. Section 2 presents a narrative review of the literature on the most important technologies that underpin Industry 4.0 and new solutions addressing the needs of Industry 5.0. Section 3 provides an overview of the Cobot use case and proposes a high-level architecture for its implementation. Section 4 presents a business-oriented view of telecom operators' capabilities in Industry 5.0, organized around three main pillars—human centricity, sustainability, and resilience—and ensuring user cybersovereignty. It pays particular attention to the role of operators in supporting and deploying Cobots. Section 5 identifies and discusses security challenges resulting from the transition to the Industry 5.0 Cobot landscape, and Section 6 summarizes the paper and presents open problems and future work.

2. Evolution of Industry 4.0 Technologies to the Fifth Generation

When presenting the robotics challenges arising from the transformation from Industry 4.0 to Industry 5.0, it is essential to consider the technologies used in contemporary industry. Typically, in industrial transformations, changes are driven by leading disciplines, which, in turn, shape the development of other manufacturing techniques and organizational structures. In Industry 4.0, these development pillars include, as shown in Figure 1, new Information and Communication Technologies (artificial intelligence, Cloud Computing, etc.), industrial techniques (additive manufacturing, autonomous robots, etc.), and organizational structures (enterprise and process integration, supply chains, etc.). Industry 5.0, in turn, is driven by new expectations to enhance the role of humans in the production process, ensure sustainable development, and ensure system resilience in the face of unexpected situations. In this section, we briefly present the most important techniques and systems that constitute the foundation of contemporary industry (4.0 and 5.0) and the impact of the recent industrial revolution on their development, with particular

emphasis on the requirements of robotics. We have conducted a narrative review of the technologies by searching electronic databases, including IEEE Xplore, Scopus, and Google Scholar, using keywords related to Industry 4.0 and 5.0 technologies. Sources were selected based on their relevance to the research objectives, with a focus on peer-reviewed journal articles, conference papers, and authoritative technical reports published primarily over the last three years. The selection process was guided by thematic relevance rather than a predefined inclusion/exclusion protocol, as the aim of this review is to synthesize current knowledge and identify technology trends rather than to provide a systematic, exhaustive inventory of the literature. Among the papers found, we selected for review those that, in our opinion, best describe the adaptation of technology to the requirements of Industry 5.0, are the newest, or are most frequently cited.

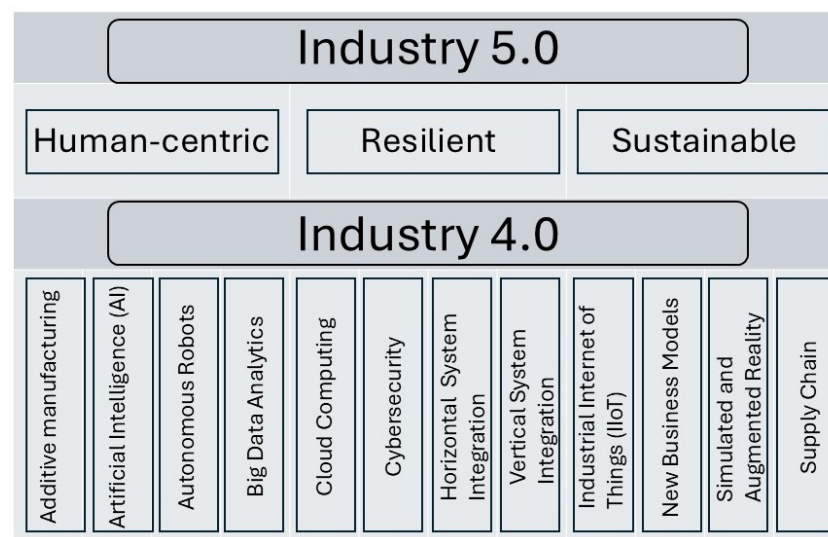


Figure 1. From the basic technologies of Industry 4.0 to the pillars of Industry 5.0.

2.1. Information and Communication Technologies Area

Nowadays, Artificial Intelligence (AI) technologies enable decision-making, large-scale data analytics, and adaptation to human creativity. For Industry 5.0, the most interesting are ethical, inclusive, and sustainable AI systems that align with human values and societal well-being. Therefore, it is not just the easy adoption of Industry 4.0 solutions; adjustments to a human-centric, sustainable approach are necessary for this concept. A recent review [14] highlights the crucial role of AI in sustainable, human-centric manufacturing within Industry 5.0 paradigms. This review identifies AI effects, including intelligent automation, greater efficiency, improved quality control, and faster decision-making. Paper [15] explores the challenges and perspectives of designing AI systems that are both human-centered and sustainable.

An approach that uses data-driven tools to enable massive data handling for optimizations and sustainability, Big Data is identified in [14] as a key enabling technology of Industry 5.0 that supports customization, faster and better decision-making, and real-time forecasting and fosters competitive pricing. An enterprise could use the Big Data approach in regular reports for management and data-driven decision-making, including automated decisions made by robot-based applications. This technology area utilizes various types of databases and storage solutions, e.g., Apache Hadoop, Apache Spark, Elasticsearch (a search engine), MongoDB/Azure CosmosDB (NoSQL database engines), and Apache Kafka/RabbitMQ (queuing/messaging systems), see [16]. Data stored in those systems could also be used in Machine Learning (ML) solutions or be provided to an AI engine as additional domain knowledge.

Like communications and teleinformatic services, Cloud services are the domain of modern telecommunications operators. For a specific Industry 5.0 application, the operator can offer various types of services, including server-based, Cloud-based, Edge-based, distributed (Fog, Dew, etc.), and mobile services with application transfer between locations [17]. They can involve using predefined “everything-as-a-Service” (XaaS) solutions [18]. Services that implement narrow Cloud and network functionalities, combined with applications delivered remotely by telecommunications operators, enable the delivery of highly specialized services designed for Industry 5.0.

The new requirements formulated in the concepts of Industry 4.0 and Industry 5.0 also place new demands on telecommunications networks, especially mobile networks. Notably, 6G networks, as a significant advancement of fifth-generation mobile networks, can meet these requirements. Numerous publications offer a vision of how 6G networks can meet the communication aims of Industry 5.0. Paper [19] outlines the most promising avenues of 6G research, as identified in the current literature. Paper [20] advocates incorporating semantic and goal-oriented aspects into future 6G networks, suggesting that this approach can lead to a significant leap in system effectiveness and sustainability. Papers [21,22] present the design of a manufacturing system that transforms Industry 4.0 into Industry 5.0, with a focus on the role of digitization and communication processes. Some papers solve specific communication problems of Industry 4.0/5.0. For instance, paper [23] addresses an application-side traffic-shaping solution for non-public networks to meet demanding transmission requirements.

Basic communication solutions include slices with parameters tailored to application requirements, appropriately secured communication connections, and networks configured to the end user’s requirements, supported by artificial intelligence methods. Paper [24] presents modern factory security from a telecommunications operator’s perspective. As required security services, it lists the following: encryption and data integrity; the privacy and security of private 5G; service resilience against failures and radio jamming; service isolation; and interoperability with existing industrial security functions. Moreover, 5G’s service-based architecture provides resilience through the redundancy of Network Functions and resources.

2.2. Manufacturing Techniques Area

Autonomous robots developed in Industry 4.0 are machines capable of performing tasks, navigating environments, and making decisions autonomously, without direct, real-time human control, see [25]. They are equipped with sensors, AI, and advanced algorithms to perceive their surroundings, process information in real time, and adapt to changing conditions. The integration of flexible and collaborative autonomous robots (Cobots) further extends the range of manufacturing services and capabilities. Cobots are designed to work together with humans, enhancing safety, dexterity, and teamwork [26]. Paper [27] provides an overview of the key stages in the transition from simple, early-stage robots (caged robots) to Cobots. They are also identified in [14] as a key enabling technology of Industry 5.0, bringing benefits such as increased productivity, robustness, enhanced dexterity, and solutions that are more consistent and accurate than those of humans.

A human–machine collaboration approach naturally supports the human-centric pillar of Industry 5.0. In this area, the focus is no longer only on task-based automation but also on objectives such as ergonomics and human safety. The idea is to shift several categories of tasks, that are repetitive, high-risk, or data-intensive, from humans to robots, which will make space for humans to focus on innovations, problem-solving, strategic thinking, etc. [28]. Another goal of the Human–Machine Collaboration is to surpass individual limits through symbiosis between the two parties [28]. Currently, humans

are the conscious partners in this collaboration, being superior to machines in decision-making and in taking responsibility. On the other hand, areas such as speed, accuracy, data processing, and monitoring are much better handled by machines.

The concept of the Internet of Things (IoT) predates Industry 5.0. However, it can still be utilized in various ways, especially in applications that interact with humans through sensors, measurements, and other means. A 2023 literature survey [29] highlights the reintegration of human and societal dimensions into IoT and Cyber-Physical Systems (CPS), marking a shift toward socio-technical Industry 5.0 systems. Also, both concepts (IoT and CPS) are related to Cobots, given the machine-like nature of the (half) Cobot. However, the idea behind Cobots is to focus on collaboration. In IoT, it is primarily about things that are interconnected but do not interact with humans much or at all. The CPS concept assumes that the Physical part of the system not only collects data as IoT devices do but also interacts with the surrounding environment. The cyber part should also be more sophisticated than in the regular IoT scenario; it could leverage advanced technologies such as Edge Computing, artificial intelligence, and automated systems. IoT was also considered in [14] as the Internet of Every Things, supporting asset productivity, cost reduction, supply chain and logistics, and enabling network intelligence. Report [30] delivered by the AIOTI organization describes the comprehensive relationship between IoT, Edge Computing, and Beyond 5G technologies, which can be used in Industry 5.0 deployments. The report describes several use cases related to these technologies, including specific network requirements.

2.3. Organization and Management Areas

New expectations for industry also enforce the use of sustainable technologies and the pursuit of a circular economy. Paper [28] considers environment, sustainability, and the circular economy as key factors in the emergence of Industry 5.0; the circular economy is also a groundbreaking research area in review [31]. Industry 5.0 changes the philosophy of progress, from a pure focus on the efficiency and speed of object and service manufacturing to a view of the industry operating in a world with limited resources. Proper resource management, including non-obvious resources such as fresh air and nature, as well as more conventional resources like energy sources and fossil fuels, is crucial [28]. Paper [32] emphasizes that solutions such as real-time data exchange and digital twins enable meticulous mapping of material flows; identification of opportunities for recycling, remanufacturing, and reutilization; and optimization of resource allocation throughout the supply chain's lifecycle. Additionally, consumers' awareness and pressure for compliance influence organizations to shift towards sustainability [33]; it is also part of a company's social responsibility and enhances workforce well-being. Paper [32] indicates that the environmental sustainability of corporations could be enhanced by optimizing the efficiency of overall resource utilization within business processes. Optimization can utilize technologies such as IoT, AI algorithms, and advanced data analytics, including Big Data.

The operating conditions of modern industry have forced collaborating organizations to integrate to leverage economies of scale in global competition effectively. Vertically integrated companies strive to organize a complete supply chain within their own organization or, at a minimum, master its key elements. Horizontal integration involves a different model of cooperation: expanding operations and extending the value chain through external partnerships (see [34]). Both of these integration models mitigate harmful competition, ensure essential collaboration, and eliminate discrepancies between supply chain components. On the other hand, excessive integration can lead to market monopolization and restrict fair competition, limiting the incentive to modernize products and production processes. Furthermore, the need to consider the human factor in Industry 5.0 makes integration trends a matter requiring special attention.

2.4. Adaptation of Industry 4.0 Technologies to the Next Generation

Beyond leveraging technologies familiar from Industry 4.0, Industry 5.0 often requires adaptation and modification, along with a strong focus on ethical use, social values, and employee well-being. Industry 5.0 will undoubtedly also leverage new and increasingly popular technological and organizational solutions (see Table 1). This technology area is primarily related to the social aspects of Industry 5.0, particularly the human-centric pillar. As paper [32] states, improving working conditions at the corporate level by introducing technologies such as AI, intelligent automation, and smart wearable will ultimately increase overall job satisfaction, employee comfort, and well-being. Additionally, organizational changes could yield positive results in this area, such as introducing remote work or flexible schedules [32]. Another key tool is leveraging the training and learning capabilities within the organization to spread desired ethical and social values, such as proper waste management, awareness of the importance of security and the human role in security frameworks, organizational resilience, sustainability, and its relation to the organization, see [35].

Table 1. The evolution of pillar technology uses in robotics from Industry 4.0 to Industry 5.0.

Pillar Technology	Industry 4.0 (Autonomous Robots)	Industry 5.0 (Collaborative Robots)
Additive Manufacturing	Useful for prototyping [36]	Useful for individual orders tailored to user needs [37]
Advanced Manufacturing	Focus on equipment connectivity, mass personalization, smart product, human intervention elimination (remote) [38]	Focus on customer experiences, hyper-customization, interactive product, human–machine collaboration (on-site) [38]
Artificial Intelligence (AI)	Trained on statistical datasets [25]	Trained on personalized and private datasets [15,39–42]
Big Data Analytics	Key technology [14,16]	The growing importance of fast-changing data for system adaptation [14]
Cloud Computing and Communication	The use of Cloud Computing and its versions (Edge, Fog, etc.) [22], 5G+ mobile networks [43], slicing [44], campus networks [45]	Cloud Continuum [46], service migration between locations [17,47], new applications [23]
Cybersecurity	Protection of industrial networks and IIoT [48], digital sovereignty [46,49–51]	Security challenges arising from the new role of the human operator, see Section 5, new technologies expected (quantum [52] and post-quantum cryptography [53]), personalized cryptography [54]
Horizontal and Vertical System Integration	The need to increase efficiency and guarantee production continuity [55,56]	Energy efficiency, circular economy, the need for individualized access to users (customers and employees) [57]
Industrial Internet of Things (IIoT)	Large-scale automation [58]	Personalized devices [59]
New Business Models	Increasing and reducing the cost of production and optimizing distribution [44,60]	Customization [61,62], cognitive solutions [39,63–65]
Simulated and Augmented Reality	Used for systems design and supporting applications [66]	Used for supporting human operators [67]
Supply Chain	Intelligent supply chain [38], agile and responsive supply chains [68]	Responsive and distributed supply chain [68], decentralized and autonomous supply chains [68]

Organizational transformation and cultural change are less directly related to technology itself; however, they support the implementation of technology and the Industry 5.0 concept in enterprises. This goal is accomplished by embedding resilience, leadership, sustainability, and human-centric values within business culture and organizational structures. In paper [69], uncertainty about new technologies and fears of job displacement were indicated as factors that strengthen resistance to those changes. Automation and human-machine collaboration are not immune to this problem. The relationships among organizational culture, explicit values, implicit norms, and unwritten rules are crucial for implementing the new paradigm. Paper [70] explores how these cultural dimensions influence behavior within organizations, impacting their readiness for Industry 5.0 adaptation.

No less important than organizational changes is the use of new technologies in Industry 5.0. An interesting technology is the concept of Digital Twins, which relates to Extended Reality (XR) [67]. A digital twin is a dynamic representation that maps a physical item to its corresponding simulation models. Paper [67] describes this concept in the context of the ISO 23247 standard for defining Digital Twins. Extended Reality (XR) encompasses Augmented Reality (AR), Mixed Reality (MR), and Virtual Reality (VR), spanning the virtual continuum between the Real Environment and the Virtual Environment [66]. Digital twins could assist operators in real-time production settings, aiming to improve sustainability, ergonomics [67], and resilience [33]. Also, Digital Twins were identified in [14] as a key enabling technology of Industry 5.0, supporting reduced costs, error prediction, design customization, and predictive maintenance. The review [66] underscores XR technologies as emerging enablers of environmental sustainability in manufacturing, which could be used for virtual prototyping, production and layout planning, ergonomic assessment, training, machine/robot interaction, cognitive support/instruction, and data monitoring/analysis.

Industry 4.0 offered the digitalization of production flows. Digitalization has enabled transparent, integrated supply chain ecosystems, erasing barriers between product development, marketing, sales, and distribution. A significant facilitator of the effective implementation of this goal is the use of blockchain technology, which implements the idea of a decentralized, mobile database, allowing for the permanent and reliable registration of transactions by independent contractors (see [71]). For instance, paper [33] suggests that system resilience in Industry 5.0, particularly in Supply Chain Management (SCM), can be enhanced by adopting technologies such as AI, blockchain, digital twins, or IoT. Those technologies could help improve the flexibility and responsiveness of supply chains, enabling SCM organizations to avoid disruptions by anticipating and implementing effective recovery measures.

The resilience of the system must be considered in both the physical and digital aspects, which might interfere with each other in some circumstances. The system could be affected by ongoing random disasters or conflicts, such as AWS Cloud services hosted in the Middle East in 2026 [72]. As a result, other regions of the AWS Cloud were also affected by workload migration. The unavailability might be caused by various factors in such an environment, from a direct strike by air attack means (rockets, missiles, drones) to a side effect of a malfunction in critical infrastructure such as power plants, transmission lines, submarine optical fiber, etc.

A cognitive system is an autonomous system that can perceive its environment, learn from experience, anticipate the outcome of events, act to pursue goals, and adapt to changing circumstances [63]. As shown, it is an integrated artificial intelligence and cyber-physical system. Cognitive systems address the need to support operators in Industry 5.0, increasing their capabilities [39]. Such cognitive assistants are key components of human-centered cyber-physical systems, especially robotic and Cobot solutions. A great support for human operators is cognitive vision technology. It helps detect an object or

event in the visual field, localize its position and extent, recognize a localized entity through labeling, and understand its role, context, and purpose [64]. Cognitivity also has its place in communications. The integration of cognitive radio and device-to-device (D2D) (so-called Cognitive D2D) communication improves spectrum and energy efficiency, increases network throughput, and enhances coverage, as shown in [65].

Customization may help with personalization, which uses technology to accommodate individual differences. Industry 4.0 introduced automation to production systems. Industry 5.0 will transform automation into manufacturing tasks, enabling consumers to acquire goods and services tailored to their specific needs (see [61]). Beyond the more sophisticated services operators could offer, the most important and simplest is ensuring direct, uninterrupted communication between the customer and the manufacturer. It enables the collection of product requirements and oversight of order fulfillment (see [62]).

Last but not least is quantum computing. It can revolutionize Information and Communication Technology (ICT) in Industry 5.0 by influencing machine learning and artificial intelligence processes [73]; solving complex optimization, simulation, and data-intensive problems [74]; and ensuring communication security [52].

3. The Shift to Cobots in Industry 5.0

3.1. The Cobot Use Case

In Industry 5.0, many use cases can be supported by collaborative robots (Cobots), which work alongside human operators in shared workspaces, combining human dexterity with robotic precision [75]. Cobots could perform tasks such as quality inspection, assembly, lifting heavy weights, or assisting in precision operations. The robot used in [75] observed humans' actions and planned its next actions, which are very basic cognitive capabilities. Additionally, Cobots continuously learn from human feedback to adjust their safety zones and motion trajectories, thereby improving collision avoidance. AI models running on Edge Cloud infrastructure enable more sophisticated, real-time adaptation to human actions and environmental changes, thereby extending the capabilities of the Cobot used in cognitive collaboration.

Communication between the Cobot and human could leverage various communication channels, from natural interfaces such as speech, gestures, a standard keyboard, or another pointing device to more sophisticated solutions such as wearables or Brain–Computer Interface (BCI). In this last option, human operators can cooperate or control Cobots directly through EEG-based brain–computer interfaces, such as the one developed in the Galea project [76]. Another way is the use of XR. Workers use XR technologies, such as AR and VR, to collaborate with AI systems supported by Cobots to make production decisions. XR interfaces provide real-time guidance and feedback to the human; for example, paper [77] describes a situation in which AR-based technologies provide visual guidance for the assembly sequence. A telecommunications operator might provide AI-based services on the Edge to support those XR systems.

All kinds of interfaces require ultra-low latency and high reliability to maintain an acceptable level of Quality of Experience for the user. Edge Cloud infrastructure, private 5G/6G networks, and AI-as-a-Service enable processing sensor data close to Cobots, reducing latency and boosting availability. Since Cobots cannot handle most complex AI tasks, delegating them to the Edge of the network might be an acceptable way to provide this service.

Unlike in Industry 4.0, where machines often operate in isolation or behind safety barriers, in Industry 5.0, the human in the loop is integral to the operation. Moreover, these Cobots must adapt to human variability (different body sizes and shapes, movement patterns, reaction times, and emotions) and to environmental changes (lighting, obstructions,

and noise). Continuous adaptation and proximity pose new risks but enable much greater flexibility, personalization of work (including customization), and worker well-being when designed correctly. The system's context awareness enables the dynamic reconfiguration of roles between humans and Cobots, e.g., if a human enters a defined safe zone, the Cobot slows or halts; if a human is fatigued, the Cobot offers assistance. This type of biometric data creates a compliance risk of improper use without the individual's valid consent. The given consent might also be abused and overused, which is called the scope creep [78].

The Cobot concept could be supported by digital and human twin technology. Industry 5.0 systems could create digital twins not only for machines but also for human operators, as described in the metaverse concept presented in the dissertation in [79]. These virtual representations enable the real-time simulation and optimization of workflows. The digital twin could represent the Cobot in the digital world, or the collaborative robot could represent the human twin in the physical world.

Below are two examples illustrating the use of Cobots.

- A medical Cobot that assists in health-related situations, starting from case management (registration, information help desk in clinic) and physical support (help with wheelchairs, stretchers, injections, simple health measurements) and extending up to the most complex situations, such as assisting in surgeries or working with emergency and rescue teams deployed to serious accidents. This kind of usage introduces several data processing and compliance challenges in the field of privacy or the processing of medical data. As stated in Section 1, we do not focus on methods for handling those challenges in this paper. Paper [38] briefly describes several ISO standards applicable to Cobots from the physical safety point of view. It also describes generic techniques used to manage the safety of the human–robot interaction—collision detection, robotic motion planning, and collaborative robot risk assessment.
- A logistics Cobot that helps humans organize and execute work in the warehouse, shop, or a constrained part of the supply chain. In contrast to the medical Cobot, this one does not pose significant ethical challenges due to errors or mistakes during daily tasks. The fundamental challenge, the prediction of the motion of collaborating humans and systems, is still valid in this example.

The next subsection contains an example architecture that supports the Cobot use case.

3.2. The Example Use-Case Architecture

In this section, we will attempt to define a use case that is both interesting to the telecommunications operator and related to the fundamental assumptions of Industry 5.0. Figure 2 shows the example architecture of the cognitive Cobot use case. The architecture utilizes the idea of the Edge network as a support for Cloud resources for providing services for the Cobot. Paper [68] shows a similar approach for generic Industry 5.0 use cases. Here, we adopt the architectural viewpoint for Cobots.

In this use case, the Cobot collaborates with humans (or multiple humans in more advanced scenarios) in a shared space and time. Both humans and Cobots can interact with their surroundings, observe them, and engage with them, essentially without any physical barriers that separate the Cobot from the human. The Cobot has limited mobility, indicating a need for a power supply system and wireless network access. Cobot should have some computing capabilities (persistent internal storage, transient internal memory, processors) to run basic functions such as object manipulation and I/O communication, including simple voice recognition and synthesis. Within the Cobot, a low-resource and low-energy AI engine could be deployed to provide simple AI capabilities, such as chatbots, within a constrained domain of knowledge.

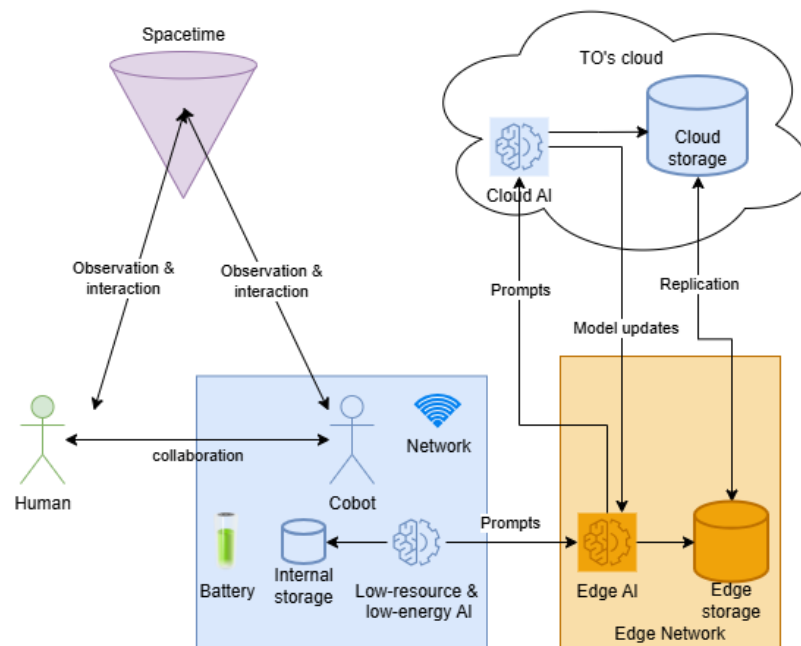


Figure 2. The example architecture for the Cobot-based use case.

Low resource and energy requirements are crucial for the proper functioning of Cobots, as current AI implementations, even domain-constrained ones, require significant storage, memory, and computational resources. Paper [47] shows how to control and manage the battery level, e.g., using backup Cobots. However, the energy management problem persists, as do side effects such as the need for proper cooling of the Cobot. As a result, real-time analysis of large sensor data, such as camera or microphone data, may not be possible directly on the Cobot and must be performed elsewhere. The AI engine can send a prompt to the Edge AI, hosted by the telecommunications operator (TO) in the Edge Network, located near the Cobot. The idea is to leverage Edge resources to deliver more sophisticated services that the Cobot itself cannot provide within the required time frame, given its limited resources. Edge AI could leverage its greater storage capacity and lack of strict energy constraints to generate answers to prompts from the Cobot. Edge AI can exchange information with the Network Operator's Cloud-based AI and Big Data engines to adjust local AI models based on current knowledge. Additionally, prompts related to the current knowledge available on the Internet might be forwarded to the Edge AI engine, which could work as a more sophisticated CDN (Content Delivery Network) service. Some simple algorithms could be executed directly on the Cobot, especially for collision management, as in paper [80]. Such algorithms require near-real-time execution, so dedicated resources (CPUs) might be needed.

From the architectural point of view, the design of communication between entities in Figure 2 requires identification of how to perform the information process. Book [81] defines the following three dimensions:

- Communication—synchronous or asynchronous.
- Coordination—based on the orchestration or choreography.
- Consistency—atomic consistency (with the ACID paradigm—Atomicity, Consistency, Isolation, Durability) or eventual consistency (the BASE paradigm—Basic Availability, Soft State, Eventual Consistency).

Book [81] describes the consequences of each combination, even for simpler examples with a narrower scope of information flows. This high-level overview does not provide final answers to those questions. However, some general guidelines could be provided for this high-level architecture.

Due to the distributed architecture, a less coupled approach is preferred here, so the communication between the Edge and Cloud entities should be asynchronous. The same applies to prompts sent from the AI deployed at the Cobot. Synchronous operations should be managed in parallel threads within a Cobot, with dedicated resources, and only for constrained, important functionalities such as basic collision avoidance.

Also, model updates and replication should use the eventual consistency model. According to the CAP theorem (Consistency, Availability, Partition Tolerance) [13], when a network partitions, the system can provide consistency or availability, but not both. That is also a reason why a Cobot should be self-sufficient in mission-critical tasks like collision avoidance or harm detection, to be able to make a safe decision even during the lack of a working connection between the Cobot and Edge or Cloud resources. Under certain circumstances, the Cobot may decide to gracefully shut itself down when services can no longer be provided in a given situation, as discussed in Section 5.3.

An interesting situation arises when determining the coordination type. Locally, on the particular information flow level, orchestration might be a better solution, because it is easier to implement the flow, especially for Edge cases. However, the Cobot might interact with other humans and Cobots within the same spacetime. Interactions between Cobots might still be implemented using the shared orchestrator, but interactions between Cobots and humans use a direct coordination pattern, which is actually the choreography approach. Due to the distributed architecture, there are the following possibilities to deploy the orchestrator:

- Directly in the Cobot—it might work for information processes that are constrained only to the Cobot and eventually communicate with the human or Edge services. However, it is naturally less error-prone than other locations. Orchestrating services located in the Cloud or on the Edge will introduce a strong coupling within the Cobot itself. So, it should be used for communicating with services that are changed rarely.
- On the Edge of the network—this location has access to Cobots and Cloud services, so it is more natural for the orchestrator. It should be easier to deploy changes in the business logic than on the Cobots.
- In TO's Cloud—deployment should be at least as easy as on the Edge; however, latency between the Cloud and Cobot could be higher.

From the deployment perspective, an orchestrator running on the Edge of the network is the easiest solution. It is also less coupled than the choreography option, in which each service included in the information process should know how to handle Edge cases and error conditions. Choreography could be an option for simple information processes constrained only to a single architecture quantum (independently deployable component, see [81]). More complex processes are easier to implement and maintain with the orchestration approach.

The described architecture may support various information flows involving the Cobot. As an example, three flows are analyzed: collision management, video communication support, and AI prompting. The first flow aims to help the Cobot detect and avoid collisions and their consequences. Edge- and Cloud-based applications could support the Cobot with physics-based calculations and the potential orchestration of other machines involved in a collision scenario. The second information flow includes voice and image recognition, analysis, and synthesis. It should enable the Cobot to understand real-time natural language input and to recognize visible humans and objects. The last flow concerns obtaining knowledge, making decisions, receiving feedback, and providing other services from AI engines, or building services such as AI agents using these capabilities. Table 2 presents the assumptions and requirements for these information flows.

Table 2. Assumptions and requirements for example information flows related to Cobots.

	Collision Management	Video Communication Support	AI Prompting
Latency	This is an example of the Ultra-Reliable and Low-Latency Communication (URLLC) services defined for 5G. Very low E2E latency and response time needed, milliseconds.	The latency and response times should be low, below a second, to enable the Cobot to conduct natural voice communication with humans and recognize them easily.	Queuing tasks are acceptable if they do not affect the collision management and basic communication interfaces with humans and other machines.
Reliability	This is an example of a URLLC service defined for 5G, where there is only a small time margin for errors, retransmissions, and decision-making processes. The system must also always be capable of handling collision scenarios, even with limited models, accuracy, and available data.	This information flow requires highly reliable services.	Due to asynchronous communication and redundant AI engines running on the Cobot, at the Edge, and in the Cloud, the required reliability level is lower than that demanded for collision management or video communication support. This architecture introduces, for this information flow, a trade-off between the quality of AI-generated responses and the required level of reliability.
Data flows	Cobot → Edge AI → Cobot and other machines.	1. Cobot → Edge AI → Cobot; 2. Cobot → Edge AI → Cloud AI → Cobot.	Cobot → Edge AI → Cloud AI → Cobot, Edge AI, and other machines.
Cobot/Edge/Cloud allocation	Operations should rely on resources available on the Cobot and at the Edge. Cloud resources might not be acceptable due to latency constraints.	Operations should rely on resources available on the Cobot and at the Edge. Cloud resources may be acceptable.	Operations should use resources available on the Cobot, at the Edge, and in the Cloud.
Fail-safe operation	Fail-safe operation must be introduced. A basic level of service must be provided by the Edge service or by the Cobot itself under all conditions.	Fail-safe operation must be introduced. A basic level of service must be provided by the Edge service or by the Cobot itself under all conditions.	Fail-safe operation can leverage the deployment of AI engines across three architectural layers (Cobot, Edge, and Cloud).
Service-level expectations	A crucial service for the Cobot; it must be provided at basic level under all conditions	Very important capability for Cobots. Image recognition should be comparable to human performance.	A fundamental service supporting the cognitive capabilities of the Cobot. A low level of hallucinations is expected.

4. The Role of Telecommunications Operators

4.1. Landscape of Telecommunications Operator's Capabilities

Industry 5.0 shifts industrial transformation towards outcomes that are human-centric, sustainable, and resilient. Telecommunication operators start from a privileged ICT position: they operate licensed, regulated spectrum and deliver deterministic QoS through network slicing and 5G network APIs. They also operate safe, reliable, and scalable communications networks and service platforms, such as those for IoT. This is supplemented by expertise in IoT devices and various communication protocols, enabling them to stay connected and exchange data with other devices and platforms. Backed by economies of scale, long-standing partnerships with trusted technology companies, and integration skills from past deployments, telecommunications operators can be especially helpful for Verticals whose core business is distant from ICT. By such cooperation, Verticals can concentrate on their core activities and manage operational risks related to ICT by transferring them to dedicated partners like telecommunications operators or equipment vendors in exchange for OPEX expenditure. The role of such partners is to provide an infrastructure tailored to the requirements of Verticals, industrial automation vendors, independent software vendors, etc. These requirements include Quality of Service, cybersecurity, data sovereignty,

and regulation. However, relying on telecommunications operators and external networks is not the only option. Verticals, with some CAPEX investment, can set up and run their own telecommunications networks, thereby becoming telecommunications operators themselves. This is possible through Vertical Spectrum Allocation, which assumes the opening of the 3.8–4.2 GHz spectrum for industrial 5G private networks. It is, first of all, an opportunity for Verticals such as manufacturing, energy, logistics, healthcare, and smart cities [82–86]. Such an approach is driven by the pursuit of eliminating vendor lock-in, fostering innovation agility, ensuring complete data sovereignty, achieving extremely low latency, and guaranteeing Quality of Service by eliminating the risk of network congestion from local public mobile traffic. Another alternative, which can be selected by the Vertical, is setting up its own WLAN Wi-Fi network with WPA3-Enterprise authentication and encryption. Activating the 192-bit mode provides the best security, suitable even in critical sectors. Traffic isolation is achieved via VLAN and SSID. The deployment of this approach is less complex than solutions involving 5G, which require specialized telecommunications skills. In general, setting up a Wi-Fi network based on widely adopted IT standards, even less protected than WPA3-Enterprise 192-bit mode, appears to be a reasonable choice for non-critical industrial applications. However, it has notable drawbacks compared to 5G, including inferior roaming and handover capabilities, which are important for on-the-move services, and reduced immunity to interference due to its use of unlicensed spectrum.

If built on standards with clear roadmaps for upgrading and integration with future networks, offerings that are telecommunication network-based aim at being as much as possible future-proof, advancing from 5G through 5G Advanced [87] towards 6G. Moreover, they can blend connectivity and computing in an “as-a-service” model across the Edge and Cloud. Multi-access Edge Computing (MEC) [88] combined with 5G enables low latency, privacy-preserving data transfer, and processing close to operations, supporting privacy-preserving use cases that put people and safety first.

Security, privacy, and sovereignty are core differentiators regardless of the operational model (own, Vertical-operated network, or delivered by an external operator). Moreover, 5G traffic is encrypted and authenticated as described in the 3GPP technical specification [89]. With hardware SIM and eSIM authentication, Subscription Concealed Identifier (SUCI) [90] for concealing the Mobile Subscriber Identity (IMSI) in transit, network slicing as a native feature, and usage of licensed spectrum, it is generally considered that they can enable secure data sharing across Verticals, in particular, for the protection of AI models trained using Federated Learning, where devices at distant locations cooperate. Thus, the models’ parameters are protected from disclosure and tampering. The additional advantage of telecommunications operators is the delivery of end-to-end cybersecurity, including operator-grade, CTI-based traffic filtering. Moreover, incumbent telecommunications operators, thanks to their engineering capabilities, possessing their own infrastructure and experience in maintaining networks, are often perceived by large enterprises and government agencies as trusted and stable organizations that can assure the resilience, business continuity, and even digital sovereignty of Verticals, as operators are subject to regulation. The latter can also be realized through network slicing and campus network deployments tailored to the Verticals’ needs (ranging from Private Access Point Name (APN) to Private Core), see [60].

Another accelerant, particularly for large networks, is 5G network APIs that let enterprises and developers embed telecommunications operators’ grade capabilities with minimal integration. The examples are network-verified location for multi-factor authentication, followed by APIs for URLLC services such as low-latency computing, uninterrupted video streaming via QoS control, or seamless XR (e.g., AR, VR) via on-demand network throughput boost [57]. These lightweight enablers compress time to market and extend the telecommunications operator’s value beyond connectivity.

With the capabilities mentioned above, telecommunication networks can drive the advent of Industry 5.0 by delivering measurable outcomes across the following three pillars:

- Human centricity: Trusted, low-latency, privacy-first solutions that empower workers and enable safe human–machine collaboration, which are the basis of Cobot services.
- Sustainability: Scalable platforms based on standards that optimize resources and support circular, cross-industry data collaboration.
- Resilience: Gardened, sovereign, and autonomous operations that are capable of maintaining continuity in business and operations under stress.

In the following subsections of this section, we show how telecommunications operators can adapt the technologies and competencies previously used to build Industry 4.0 to the needs and requirements of Industry 5.0.

4.2. Contribution to Human-Centricity Pillar

Even using existing 5G Public Land Mobile Network (PLMN) with its five pillars, which are enhanced Mobile Broadband (eMBB), URLLC, massive Machine Type Communication (mMTC), energy efficiency, and network slicing, a telecommunications operator can offer customized services to Verticals. It can be achieved, in the first place, through network slicing, which is possible with stand-alone 5G implementations that, unlike non-stand-alone ones, include the 5G Core. Using an identifier called Single-Network Slice Selection Assistance Information (S-NSSAI) (see [44,91] for a blockchain-based solution), a network slice dedicated to devices belonging to a particular Vertical can be distinguished. In such a network slice, a required Service Level Agreement (SLA) can be fulfilled. In case of implementations in specific locations, telecommunication operators can go beyond that in service customization by providing connectivity over Private Networks and, in particular, Campus Networks [45], which are deployed within a limited, defined geographical area, e.g., a logistics or production facility. These networks can offer even more privacy and sovereignty for safer, smarter work and can be a major driver of digital transformation by combining voice and data connectivity with computing, data storage, and cybersecurity. A comparison of characteristics of various models of network offerings is shown in Table 3.

Campus networks are implemented using licensed spectrum, free of the interference common in unlicensed networks. They create a safe nest for interconnecting various devices, including routers, tablets, smartphones, VR and AR headsets, laptops, and numerous IoT devices, e.g., sensors. They can be further supplemented with various tools, enablers, and applications, such as IoT platforms; security solutions, e.g., firewalls supported by Cyber Threat Intelligence (CTI); low-latency critical communication for Cobot control; drones for security monitoring; asset tracking; and various applications of video for security, infrastructure inspection, and quality control. Verticals can benefit from telecommunications operators' experience in deploying and operating such networks, including network planning and design, hardware delivery and installation, integration, and configuration. Once the network is set up, the operator can offer network monitoring, on-site support, and end-to-end performance and security checks, in accordance with the applied SLA. By choosing the desired deployment model, a perfect balance can be achieved between sovereignty, privacy, and cost that is optimal for the specific business of a particular Vertical.

There are various models of Campus networks. The simplest one assumes that a gNodeB (gNB) is located on Vertical's premise and Vertical receives a Private APN. Thanks to that, the Vertical's data is logically separated from other traffic. Other intermediary variants shift various network components to the Vertical's premises, starting with the User Plane Function (UPF), which improves privacy by routing data locally within the campus network. It can be followed by further moving network functions to the Vertical's premises for even greater privacy. Finally, a solution called Private Core can be offered,

in which all core network elements are located at the Vertical's premises. In such a case, the Vertical also gains control over provisioning, billing, SIM management, and compliance with legal requirements, e.g., data retention and lawful interception. Obviously, the most advanced, non-public variants of 5G Stand-Alone (SA) campus network realizations are well suited for supporting human-machine collaboration thanks to privacy, deterministic QoS, precise indoor positioning for worker geofencing, and people-aware Automated Guided Vehicle (AGV) and Cobot zones. Campus networks have already undergone field trials and implementations in the areas of innovation, industry, and critical infrastructure. Notable examples include the LTE and 5G networks in the LSSE special economic zone, which promote innovation. These networks support acceleration programs for startups utilizing 5G technology to develop advanced services [92]. Another example is the 5G network designed for industry, built in a household appliance factory, to enable several complex services, such as AGV, massive IoT deployments, and remote expert support using AR [93]. An example of 5G deployment in critical infrastructure is the implementation in Le Havre, France's leading container port. The network was established to serve various use cases—from Smart Cruise, which improves the flow of people and goods, to autonomous shuttles operating between the port and the city, and drone-based incident detection [94]. The technical scope and operating model of such implementations vary according to the customer's requirements. Typically, they include small cells (femtocells, picocells, and microcells) to provide full coverage, as well as edge servers for on-premises data storage and processing. These may be complemented by core network elements where required. From an operational perspective, licensed spectrum is most often provided by the telecommunications operator, while equipment maintenance may be delivered either by the operator or by the equipment vendor.

Mobile networks, public or private, backed by telecommunications operators' Edge Computing capabilities, enable advanced use cases. In particular, MEC facilitates the implementation of AR and VR for training and assistance. Such networks align well with addressing one of the challenges of implementing Industry 5.0: the large scope and high cost of workforce training. A cost reduction is achieved by avoiding the use of real infrastructure for training, thus reducing downtime and speeding up personnel onboarding. Moreover, further savings can be achieved through real-time speech services that reduce people's errors and facilitate human-machine cooperation.

Safety of employees can be enhanced by providing them with Personal Protective Equipment (PPE). These can take the form of network-connected wearables equipped with accelerometers and biometric sensors for accident detection, and for indoor and outdoor positioning. PPE can be bundled with mission-critical voice, video, and data, as well as AI-based Edge computer vision, for incident prevention and response. All these are in line with human-machine interface modernization, which includes haptics (tactile feedback, force feedback), closed-loop control via URLLC, usage of Time-Sensitive Networking (TSN) integrated with Precision Time Protocol (PTP) [95] for safer aligning the clocks of all connected devices across the network, achieving the precision and accuracy necessary for Cobot operations that prioritize human safety, ergonomics, and comfort.

Furthermore, all these technologies significantly support the Human-centricity pillar of Industry 5.0 by offering privacy-preserving analytics thanks to on-premises computing resources and data storage for sovereign analysis and enhancement of AI models through federated learning for efficient finding of insights, allowing for faster time-to-competency, reduced downtimes, and improved worker satisfaction, while protecting workers' data.

Table 3. Comparison of characteristics of a 5G/LTE Campus Network, Network Slice in a 5G Network, and a Public 5G/LTE Network.

	5G/LTE Campus Network	Network Slice in a 5G Network	Public 5G/LTE Network
Network resources	Dedicated network resources reserved exclusively for the customer	Logically dedicated resources allocated by the operator for a specific customer or service, while running on shared public network infrastructure	Shared public network resources used by multiple customers
Network coverage	Private coverage designed for the customer site, including strong indoor coverage; access limited to authorized customer devices	Available within the operator's public 5G coverage area; coverage and indoor performance depend on the public radio network, but can be optimized for specific service needs	Coverage provided by the public mobile network; indoor performance may be limited in some locations and dead zones may occur
Data rate	High, stable, and predictable throughput with dedicated capacity	More predictable and prioritized performance than standard public service; actual throughput depends on slice design and radio conditions	Shared capacity with variable and less predictable throughput, especially during periods of congestion
Latency	Low and predictable latency, typically ranging from 1 ms to 20 ms	Lower and more consistent latency than standard public mobile service; can be configured for low-latency use cases depending on the service design	Variable and less predictable latency, typically 20 ms or higher
Antennas	Typically based on indoor small cells deployed on the customer premises	Uses the operator's public 5G radio network, typically based on macro cells and, where available, small cells	Typically based on public outdoor macro cell sites
SIM cards	Usually dedicated SIM cards configured specifically for the campus network	Operator SIM cards enabled for access to a specific network slice or service profile	Standard operator SIM cards used for public mobile services
QoS and prioritization	The customer can define user access, resource allocation, and traffic prioritization policies	Predefined or guaranteed QoS profiles with traffic prioritization and service differentiation managed by the operator	Best-effort service with no dedicated QoS guarantees; performance may degrade for all users during congestion
Connection density	Supports high device density, including thousands of devices on the customer site	Can support high device density depending on slice configuration and available radio capacity	Capacity is shared among all users connected to the cell and may be limited in dense environments
Data sovereignty	Sensitive data is typically processed and stored locally on the customer premises	Traffic can be logically separated; depending on the architecture, data may use dedicated operator core functions, but is typically not processed fully on-premises	Data is transported through the operator's core network before reaching application servers or destination systems
Maintenance and upgrades	Planned and controlled by the customer	Planned and managed by the operator, typically in line with agreed service levels	Planned and managed by the operator

4.3. Contribution to Sustainability Pillar

Existing mobile networks, both 4G and 5G, can support Sustainability. Energy-efficient IoT communication standards such as NB-IoT, LTE-M, or 5G Reduced Capability (Red-Cap) [59] can be used to connect sensors cost-effectively. Such sensors can monitor energy consumption in real time, in line with ISO 50001 [96]. Moreover, they could detect water, compressed air, or heat leaks for automated detection and response. Combined with MEC analytics, this can provide insights to optimize the operating parameters of industrial processes and heating, ventilation, and air conditioning (HVAC) systems.

Mobile networks also enable the development of remote operations that cut emissions by using drone and robot inspections controlled over 4G or 5G networks. Telepresence and remote condition monitoring reduce site visits across distant locations.

Moreover, PLMNs can be used for the supervision of sustainable supply chains, where IoT devices can monitor asset condition during transportation and track the provenance of goods, e.g., ensuring that cold-chain integrity is maintained, thus supporting waste reduction and circularity. It is worth noting that services on the move, under certain conditions, may encounter latency issues. For services with strict latency requirements, migrating the application from the current Edge node to a closer one could be the remedy. Such real-time migrations are not easy to realize. However, research is underway within the Computing Continuum area. It includes works on application orchestration, a common abstraction layer for platform-agnostic application execution, and assurance of sovereignty over data during and after migration.

Telecommunication operators themselves care about sustainability. The examples include gradual replacement of traditional SIM cards with eSIMs, device take-back programs, and energy efficiency in Radio Access Networks (RANs). It is estimated that the network energy efficiency of 5G is two orders of magnitude better than in 4G, and it is expected to be twice as good in future 6G as it is in existing 5G networks [97–100].

4.4. Contribution to Resilience Pillar

In the area of connectivity, telecommunications operators go beyond PLMN. Thanks to their integration skills, telecommunications operators can provide hybrid, always-on access via fiber, 5G, and Non-Terrestrial Networks (NTN) using satellite constellations for global coverage. Further hardening can be achieved through dedicated network slices, e.g., for Operational Technology (OT), to keep it separated from external factors and ensure the production process remains up and running. Moreover, local autonomy with MEC enhances resilience, as the plants can continue operating even when external communication fails. Telecommunication operators' 24/7 Security Operations Center (SOC) could provide cybersecurity services for Vertical's OT systems, and MEC could host Edge-based anomaly-detection solutions. At the same time, SIM and eSIM could securely implement zero-trust in OT for device onboarding, even across multi-vendor fleets. Advanced cybersecurity monitoring, detection, and response are crucial for improved disaster recovery readiness and compliance with regulations, e.g., the Network and Information Systems Directive 2 (NIS2), which covers a broader list of Important Entities (IE) and Essential Entities (EE) than previous regulations [101].

Telecommunication operators can help ensure supply and operational continuity using IoT. It enables predictive maintenance through analytics of data collected by sensors and digital twins, as well as work-in-progress, finished goods, and spare parts. Thanks to connectivity and on-site computing power, multi-site failover strategies can be prepared and implemented. Moreover, emergency communications can speed up incident response and evacuation.

4.5. Service Scenario Patterns and Opportunities

By aligning their offerings with these three pillars, telecommunications operators can move beyond connectivity to deliver measurable outcomes—safer workplaces, lower environmental impact, and robust, interruption-tolerant industrial operations. It could come in the form of a general, “as-a-service” business model that encompasses private 5G and Wi-Fi, MEC, security solutions, IoT platforms and devices, and analytics. The examples of such service scenarios are as follows:

- Human Safety and Assistance service scenario that includes campus network, PPE wearables, and Edge Computing for privacy-preserving analytics.
- Energy and Carbon Optimization service scenario that utilizes IoT energy consumption metering and waste detection, and AI-controlled management for the most efficient usage of production equipment and HVAC systems as well as green SLA automated reporting.
- High-availability Resilient Operations service scenario that bundles hybrid connectivity, slicing, OT security assured by SOC, and high-availability, redundant Edge, and Cloud.

It could be further fine-tuned to the needs of particular Verticals by means of appropriate partnerships with independent software vendors and OT vendors for co-development and subsequent offering of pre-integrated blueprints for specific vertical industries, e.g., manufacturing, utilities (electricity, gas, water, sewage, and waste), logistics and transportation, healthcare, etc. Another opportunity is related to Application Programming Interface (API) exposure, e.g., multi-factor authentication, location, QoS on demand, and so on. Furthermore, telecommunications operators can leverage their expertise in compliance to support verticals with continuous compliance reporting, e.g., under the General Data Protection Regulation (GDPR) and NIS2. Finally, they can also use their experience in customer care automation to further enhance the human–machine interface and collaboration.

4.6. Contribution to Digital Sovereignty

Generally, the cyberspace sovereignty of a state is based on the ICT systems under the state’s own jurisdiction. Cyberspace sovereignty is exercised to protect IT systems and various data operations within the country’s borders. In cyberspace, these boundaries are determined by the border elements of a country’s computer network (device ports, network gateways, etc.) and by the network devices of other countries [46]. In practice, digital sovereignty is based on three pillars [49]:

- Data sovereignty: Customers need a mechanism to prevent providers from accessing their data unless customers explicitly approve access for specific provider behavior, because they believe the access requests are necessary. In this domain, telecommunications operators can provide all known data protection measures typically offered to protect data in transit and at rest. A spectacular solution that ensures users meet national legal requirements for handling protected data is to place Cloud Computing within a defined, territorially limited legal area; see, for example, [50].
- Operational sovereignty: Depending on the industry that an organization operates in, there might be a requirement for further controls. With these capabilities, the customer benefits from the scale of a multi-tenant environment while preserving control similar to a traditional on-premises environment. In the case of AI-powered systems, a key element of control is the provision of proprietary AI solutions, including the protection of training data, the definition of evaluation schemes, and the prioritization of results (see [41]). Telecommunications operators play a crucial role in this domain.

- **Software sovereignty:** Users have access to platforms that embrace open APIs and services. Also, they have access to technologies that support the deployment of applications across many platforms in a full range of configurations. Telecommunication operators have the full right to advise end-users to use only trusted applications and, in cases where legal restrictions on the use of specific programs and devices apply, to prevent their implementation [51].

Ensuring digital sovereignty for Cobot services during both implementation and operation, and migration remains an important security issue required of a telecommunications operator.

Figure 3 shows another aspect of digital sovereignty. In the landscape of organizations, clients, vendors, states, international organizations, and others, there are relationships among those entities. Through those relationships, entities are trying to enforce particular behavior on other entities in the context of digital operations. The Network Operator plays a vendor role for the organization and might provide solutions that help the organization in the area of digital sovereignty, but might also impose limitations on the organization's digital sovereignty. It might, e.g., be a requirement to use dedicated network hardware, to adhere to throughput limits, or to limit cellular network coverage.

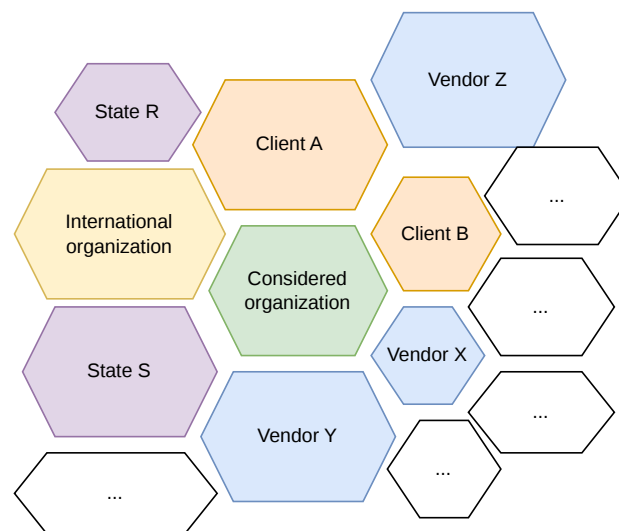


Figure 3. Impact on the digital sovereignty of the organization.

5. Emerging Security Challenges

5.1. Differences in Security Challenges Between Industry 4.0 and Industry 5.0

Although the security challenges for Industry 4.0 and 5.0 appear similar (both primarily use the same technologies and concepts), the differences arise from their definitions and the degree of human orientation [48,102,103]. Industry 4.0 robotics focuses on automation, efficiency, and the separation of humans from the process (humans can only control the work). Industry 5.0 robotics (Cobots) concentrates on human–robot collaboration, adaptability, and trust, see Figure 4.

With this in mind, threats evolve from typical technical risks to more complex technical, human, and ethical risks, making risk management in Industry 5.0 both more advanced and more critical. These differences are presented in Table 4.

Threats related to the exploitation of known and popular vulnerabilities exist in both Industry 4.0 and 5.0. However, in the case of Industry 4.0, the threats mainly focus on technological vulnerabilities (e.g., outdated software versions or unauthorized access to devices/systems). In Industry 5.0, there are additional vulnerabilities related to AI (e.g., model poisoning), the Cloud Continuum, and systems supporting direct human interaction.

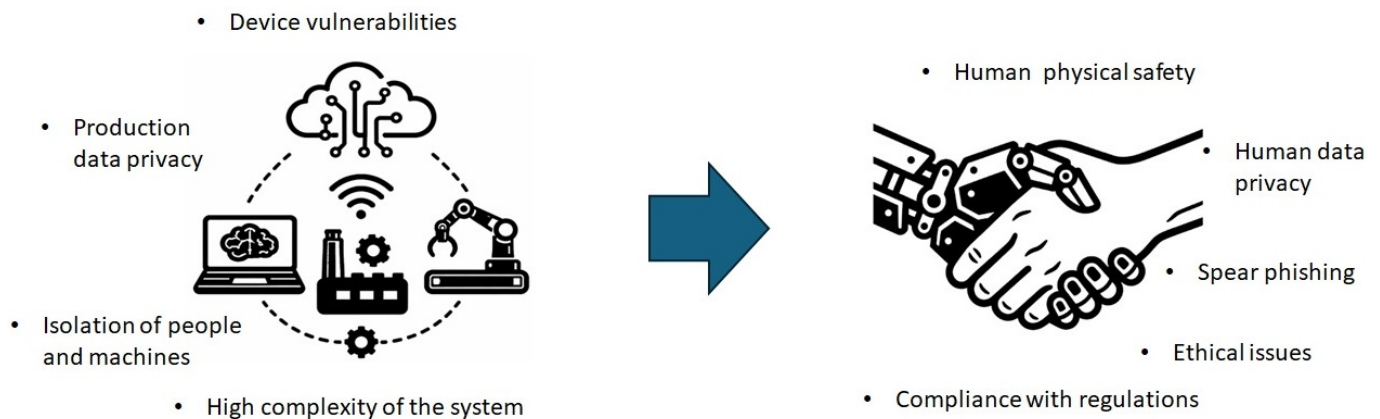


Figure 4. Shifting the burden of risk from devices to people.

Another security challenge is managing data and ensuring its secure storage. In Industry 4.0, data primarily consists of production data collected by robots and related process parameters, along with their analysis and real-time transmission. Industry 5.0 extends this scope of data through its human-centric approach [104]. Cobots can therefore collect biometric data on operators (often including data related to their current state of health), their behavior, gestures, and voice, which significantly expands the scope of information protection.

The complexity of Industry 5.0 systems also poses significant security challenges. In this case, system integration involves not only connecting Cobots to SCADA, IoT, or emergency systems but also to solutions that use ML/AI, digital twins, or interfaces for direct human interaction. This approach significantly increases the attack surface, extending it to include new threats associated with new technologies and their integration with “classic” systems.

Another category of safety challenges is physical safety. While in Industry 4.0, robot protection mainly focused on isolation and remote control, in Industry 5.0, due to its proximity to humans and shared workspaces, dynamic physical safety is required to protect both the Cobot and the operator. Yet another security challenge stems from one of Industry 5.0’s pillars: customization. The customization of the production process and its mass scale can introduce and replicate security threats that, if not detected early, will be difficult to remedy.

Another important group of safety challenges associated with the use of Cobots in Industry 5.0 is AI [42]. Attackers manipulate the data used to train AI models, leading to incorrect decisions. Moreover, hackers can feed manipulated input data to deceive AI algorithms (e.g., by slightly altering the image to fool a human gesture recognition system). Additionally, another challenge includes attempts to steal or reverse-engineer AI models to replicate or exploit their functionality. Protection against such scenarios is particularly crucial in the context of advanced AI applications in Industry 5.0.

Phishing is also an important challenge in Industry 5.0. Due to the widespread use of generative AI, phishing has become increasingly effective and has also changed in nature, as can be observed in Industry 5.0. Given the close interaction between humans and Cobots, all forms of spear phishing and deepfake (Deepfake Voice Cloning and Deepfake Video Calls) pose a significant challenge, as they can lead to production line stoppages or the execution of commands by a fraudster impersonating a manager (e.g., altering a Cobot’s normal movement path due to new tests being carried out).

Table 4. Comparison of security challenges for Industry 4.0 and Industry 5.0.

Security Challenge	Impact on Industry 4.0	Impact on Industry 5.0	Key Differences Between the Two Concepts
Cybersecurity vulnerabilities	Risks associated with accessing the robot via PLC controllers, IoT, and remote communication interfaces	Increased attack surface of Cobots through sensors, wearables, Cloud Continuum, AI, and direct human interaction	The transition from a device-oriented approach (Industry 4.0) to a human-oriented approach (Industry 5.0) has led to an increase in risks in Industry 5.0
Data privacy	Limited to production data, robot telemetry, and process parameters	Contains worker biometric data, motion tracking, voice, and behavioral data captured by Cobots	Shift from device-centric to human-centric data privacy protection and ethical data handling
Systems integration	Integration of robots with systems such as ERP, SCADA, and vision systems	Extending the integration of Cobots with systems using AI, digital twins, and human interfaces	Increasing the attack surface in Industry 5.0 through integration with new types of systems
Physical safety	Static safety ensured by isolating equipment (e.g., cages, light signals)	Dynamic safety required for close collaboration between humans and robots and shared workspaces	Industry 5.0 replaces physical separation with adaptive safety mechanisms
Customized production processes	Robots enable mass customization by flexible automation and adaptation	Cobots support a high level of customization by combining human creativity with robotic precision	A high level of customization and flexibility may result in the unintentional replication of threats
AI vulnerabilities	AI used for interpreting and reacting to visual data from robotic surroundings, path planning, and predictive maintenance	AI supports decision-making, learns from humans, and enables human–robot collaboration	Human trust in robots in Industry 5.0 depends on the performance and reliability of the AI algorithms used
Phishing	Acquisition of data enabling access to IT/OT systems; loss of access to services due to a ransomware attack	Forcing a Cobot to perform specific actions (e.g., changing its pre-set movement path or updating its software)	In Industry 4.0, the target of an attack is mainly the system; in Industry 5.0, it is the human
Regulatory and compliance	Compliance with machine (robot) safety standards and data protection	Compliance with machine (Cobot) safety standards and data protection extended to include ethical and legal aspects, as well as workers' protection	In addition to safety standards related to devices and processed data, Industry 5.0 adds aspects related to ethical issues (e.g., the use of AI) and social issues (direct cooperation with humans)
System complexity	High complexity of systems resulting from the operation of multiple robots and control automation	Very high complexity of systems due to the addition of dynamic adaptation, cooperation, and learning factors	Industry 5.0 introduces more complex systems that focus not only on technical aspects, but also on social ones
ROS threats	Vulnerabilities in ROS affect the autonomy of robots, their communication, and the correct functioning of the entire environment in which the robot is used	Vulnerabilities in ROS directly affect the life and safety of workers due to the nature of cooperation between humans and Cobots and sharing common spaces	In Industry 5.0, the risks associated with ROS are not only operational in nature but also have a direct impact on the health and lives of operators

An equally important group of security challenges in Industry 5.0 is those related to regulations and compliance. In addition to meeting technological standards for robots, several ethical, social, and data protection issues must be considered. It makes compliance with these regulations quite complex, time-consuming, and complicated.

Whereas in the case of Industry 4.0, Robot Operating System (ROS) [105] affects the autonomy of robots, their communication, and the correct functioning of the entire environment in which the robot is used, in Industry 5.0, they can have a direct impact on the health and lives of workers sharing the same space as the Cobot.

Of course, the security challenges for robots and Cobots listed earlier are the most significant, but they also highlight the complex security challenges that need to be addressed in Industry 5.0.

At the same time, it should be emphasized that the listed security challenges vary in nature (e.g., direct cyber threats, direct physical threats, and challenges that increase potential security risks) and, consequently, have varying significance on industrial systems (see Table 5). Table 5 illustrates the impact of security challenges on robots and Cobots in Industry 4.0 and Industry 5.0, respectively. As can be seen, security challenges in Industry 5.0 have a noticeably greater impact than in Industry 4.0. Furthermore, the challenges directly related to human–Cobot collaboration—namely, physical safety risks and ROS (including robot software issues)—are critical. It is because they can directly affect the health of the Cobot operator (particularly when the Cobot is unfamiliar with a procedure, does not know how to behave, or performs its tasks incorrectly). Other challenges also have a significant impact, although those relating to regulatory and compliance issues are of the least concern, as they cannot directly compromise systems or safety or cause immediate operational disruption (instead, they may delay, restrict, or block the use of Cobots).

Table 5. Security challenges and their significance in Industry 4.0 and Industry 5.0.

Security Challenge	Type of Challenge	Industry 4.0 Significance	Industry 5.0 Significance
Cybersecurity vulnerabilities	Direct cybersecurity threat	High	Very High
Data privacy risks	Direct cybersecurity and data protection threat	Medium	Very High
Systems integration failures	Technical cyber-physical operational threat	High	Very High
Physical safety risks	Safety-critical operational threat	High	Critical
AI vulnerabilities	Direct cybersecurity threat	Medium	Very High
ROS	Direct cybersecurity threat	High	Critical
Phishing attacks	Social engineering/Human-layer cyber threat	High	Very High
Regulatory and compliance issues	Governance and compliance constraint	Medium	High
System complexity	System-level risk amplifier	High	Very High
Customized production process misconfigurations	Risk exposure amplifier	Medium	Very High

5.2. Compact Security Threat Mapping for Industrial Robotic Systems

To systematically identify, assess, and prioritize potential threats, a high-level threat model (a conceptual threat modeling abstraction rather than a formal model) has been developed, as shown in Table 6. This Table includes six security challenges, which are the most representative or critical threats, namely, cybersecurity vulnerabilities, data privacy risks, physical safety risks, AI vulnerabilities, ROS threats, and phishing attacks. The remaining challenges, namely, system complexity, customized production processes, regulatory and compliance issues, and system integration failures, are system-level factors

that influence the security posture of industrial robotic systems rather than stand-alone threats. In addition to the security challenges themselves, Table 6 provides information on affected assets (what is the target), threat actor(s) (who is responsible), attack vectors (how an attack can be performed), and potential consequences (what might happen). It should be emphasized that this model does not include a quantitative assessment of a given threat (such as severity), as, in this case, the decision was to focus on qualitative characteristics and a system-level understanding of security vulnerabilities. In particular, the impact of a given threat on Industry 4.0 and Industry 5.0 is shown in Table 5.

Table 6. Compact threat model for industrial robotic and collaborative robotic systems.

Security Challenge	Asset(s)	Threat Actor(s)	Attack Vector	Consequence
Cybersecurity vulnerabilities	Robots, controllers, networks	External attacker, insider	Malware, exploits, unauthorized access, misconfiguration	Production disruption, system compromise
Data privacy risks	Operational and employee data	External attacker, insider	Data breaches, unauthorized access	Privacy loss, theft of intellectual property, regulatory penalties
Physical safety risks	Human operators, Cobots, equipment	Attacker, system error, operator	Sensor spoofing, robot manipulation	Injuries, equipment damage
AI vulnerabilities	AI models, decision systems	Attacker, malicious data source	Data poisoning, adversarial inputs	Unsafe or incorrect decisions
ROS	Robot controllers, ROS nodes	External attacker, insider	Node compromise, message spoofing	Loss of robot control, disruption
Phishing attacks	Human operators, engineers	Social engineer	Credential theft, phishing emails	Unauthorized system access

5.3. Security Challenges from the Perspective of the Pillars of Industry 5.0

Naturally, security can be viewed from various angles, especially in the context of human–Cobot collaboration. In particular, it is important to address the security challenges associated with Industry 5.0 (see Table 7).

Table 7. Security challenges for Cobots in the context of Industry 5.0 pillars.

Industry 5.0 Pillar	Security Challenge
Human centricity	Physical safety risks from cyber attacks
	Privacy breaches of worker data
	Trust erosion via spoofing
	Ethical AI vulnerabilities
Sustainability	Supply chain attacks on eco-materials
	Energy manipulation attacks
	Lifecycle tampering
	Environmental sensor spoofing
Resilience	Single point of failure in networked Cobots
	Denial-of-service on real-time operations
	Supply chain resilience breaches
	Recovery manipulation

The human-centric pillar emphasizes seamless and safe collaboration between humans and machines, placing people at the heart of automation. This vision relies on Cobots adapting in real time to individual workers' movements, preferences, and even emotional states. However, this close integration creates vulnerabilities, such as physical safety risks from cyberattacks, in which attackers could remotely alter Cobot behavior (overriding safety protocols or falsifying sensor data) to cause dangerous movements near workers, turning a collaborative partner into an unwitting hazard. Another concern is the potential for privacy breaches of worker data, as Cobots continuously monitor gestures, biometrics, voice patterns, and performance metrics to personalize interactions. Without strong encryption and access controls, this sensitive information becomes a major target for unauthorized access, corporate espionage, or identity theft. Additionally, trust erosion via spoofing poses a subtle but profound threat when attackers mimic legitimate human inputs (using forged signals, deepfake gestures, or manipulated voice commands) to deceive the Cobot into executing unsafe or incorrect actions, gradually eroding operator confidence in the system. Finally, ethical AI vulnerabilities arise when biases embedded in machine learning models are deliberately exploited, potentially leading to discriminatory task assignments, exclusion of specific demographics, or unfair performance evaluations, thereby undermining the inclusive and equitable intent of human-centric design and risking workplace morale and legal liability.

Under the sustainability pillar, Cobots are designed to support eco-friendly, resource-efficient manufacturing, aligning with the principles of the circular economy. However, this green focus opens the door to supply chain attacks on eco-materials, where compromised components, especially those made from recycled or bio-based sources, might contain hidden backdoors, counterfeit firmware, or tampered sensors that enable large-scale sabotage of environmentally aligned processes. Energy manipulation attacks are also a growing risk, with hackers forcing Cobots into inefficient operational loops (such as repeated idle motions or redundant calibrations) that waste electricity and contradict corporate sustainability targets. Lifecycle tampering becomes a critical concern when remote intrusions alter Cobot firmware to turn off diagnostic tools, block modular upgrades, or prevent proper end-of-life recycling, thereby accelerating electronic waste and undermining long-term environmental responsibility. Moreover, environmental sensor spoofing allows attackers to falsify real-time data on emissions, energy use, temperature, or material consumption—either to mask unsustainable practices during audits or to trigger false compliance alerts that divert resources from genuine green initiatives.

The resilience pillar focuses on systems that can withstand, adapt to, and recover from disruptions (whether technical failures, cyberattacks, or supply shocks). Resilience is also an important challenge in Industry 5.0 due to the dynamic nature of cooperation with operators; Cobots should operate reliably while remaining flexible for potential reconfiguration. Another important aspect is to establish rules for Cobot behavior in the event of unstable operation (including requirements related to graceful shutdown). Despite this focus, a single point of failure in networked Cobots remains a critical weakness, especially in highly interconnected swarm configurations, where a compromised unit can spread malware laterally across the fleet via shared networks, over-the-air updates, or synchronized AI models. Denial of service on real-time operations threatens continuity by jamming wireless communication channels, flooding Edge processors with junk data, or triggering emergency stops altogether—halting adaptive responses precisely when flexibility is needed most during production crises. Supply chain resilience breaches occur when third-party software libraries, sensors, or Cloud services introduce undetected vulnerabilities (such as zero-day exploits or weak authentication) that bypass redundancy mechanisms and turn off backup systems. Lastly, recovery manipulation targets failover

protocols, self-healing AI features, and digital twin simulations, deliberately corrupting restore points or injecting delays to prolong downtime, amplify financial loss, and erode stakeholder trust in the system's robustness.

5.4. Impact of Security Threats and Challenges on Entities Involved in Cobot Collaboration Services

Based on the example architecture for the Cobot-based use case mentioned in section three, we can see that the service involves several stakeholders:

- User, who interacts directly with the Cobot.
- Telecommunications operator, who provides communication links and, where applicable, Edge Computing.
- Cloud Computing service provider.
- Cobot.

Each party is exposed to specific risks discussed earlier in this section. Table 8 analyzes the Impact of a given security challenge on a stakeholder (who is at risk) and indicates which party should take measures to mitigate the risk in order to eliminate or minimize the associated risk.

Table 8. Impact of security challenges and threats on Cobot use-case stakeholders.

Security Challenge	Affected Stakeholders	Stakeholders Responsible for Risk Mitigation/Minimization
Cybersecurity vulnerabilities	user, telecommunications operator, Cloud Computing service provider, Cobot	telecommunications operator, Cloud Computing service provider, Cobot creator (both software and hardware)
Data privacy	user, Cloud Computing service provider	telecommunications operator, Cloud Computing service provider
Systems integration	telecommunications operator, Cobot	telecommunications operator, Cobot creator (both software and hardware)
Physical safety	user	telecommunications operator, Cobot creator (both software and hardware)
Customized production processes	telecommunications operator, Cobot	telecommunications operator, Cobot software creator
AI vulnerabilities	user, telecommunications operator, Cloud Computing service provider, Cobot	telecommunications operator, Cloud Computing service provider, Cobot software creator
Phishing	user	telecommunications operator, Cobot software creator, user
Regulatory and compliance	telecommunications operator, Cloud Computing service provider, Cobot	telecommunications operator, Cloud Computing service provider, Cobot creator (both software and hardware)
System complexity	telecommunications operator, Cobot	telecommunications operator, Cobot creator (both software and hardware)
ROS threats	Cobot	Cobot software creator

The first category of risks consists simply of cybersecurity vulnerabilities, and all parties involved in the service are exposed to them (depending on the type of vulnerability). Consequently, mitigation is the responsibility of those parties that are technically capable of detecting and defending against these threats, namely, the telecommunications operator, Cloud Computing service provider, and Cobot creator (including software and hardware developers). Phishing constitutes a distinct threat group here, to which users interacting

with the Cobot are particularly vulnerable. However, here too, the telecommunications operator, the Cobot software creator (the Cobot should be able to detect certain forms of deepfake phishing), and the user—who should be highly aware of such activities and able to distinguish a genuine email from a fake one—should be responsible for detecting and blocking such activities.

In the context of data protection, the vulnerable parties are those that are the direct source of the data (the user and the Cobot) or those that store the data (the Cloud Computing service provider). In this case, it is necessary to ensure appropriate access management for this data, as well as a sufficient level of encryption during transmission and at rest, which the telecommunications operator and the Cloud Computing service provider can provide.

Another significant security challenge is the integration of systems in this use case, and this integration will have the greatest impact on the telecommunications operator (ensuring communication between the various elements of the Cobot ecosystem) and the Cobot itself, which will need to be connected and work with many components to provide the service correctly. Taking these assumptions into account, the telecommunications operator and the Cobot developer (in both software and hardware) will be responsible for the secure, uninterrupted integration.

Given the principle of direct collaboration between the user and the Cobot, which is a fundamental pillar of Industry 5.0, the user is at risk of physical injury caused by the Cobot (e.g., as a result of a malfunction). In such cases, the telecommunications operator is responsible for procedures such as a graceful shutdown, in which the Cobot is safely switched to a standby mode where it will not perform its normal functions. The Cobot's developers should enable such a scenario to be programmed.

Another challenge relates to adapting the production process. Each client may require a different set of operations and actions from the Cobot (and, indirectly, from the telecommunications operator). Furthermore, the complexity of the environment in which the user will work with the Cobot may increase associated risks. Given the uniqueness of each such case, risk mitigation should be the responsibility of both the telecommunications operator and the Cobot software developers.

A significant security challenge lies in AI-related risks. Artificial intelligence is developing rapidly, and as a result, new risks are emerging that affect all parties involved in the service. In turn, it requires risk mitigation on multiple fronts by the telecommunications operator and the Cloud Computing provider (which may supply computing resources for the ML process), and the Cobot software developer, who can protect against specific attacks.

Of course, given the novelty of the human–Cobot collaboration service, it is necessary to comply with all relevant regulations and requirements to ensure the entire use case can legally provide the service. They apply in particular to the telecommunications operator, the Cloud Computing provider, and the Cobot developer, who are responsible for meeting the necessary legal standards.

The final security challenge discussed, which may pose risks, relates to the robotic operating system (ROS). Cobots are vulnerable to these risks, and it is Cobot designers, together with the developers of the relevant ROS, who should mitigate the risks posed by significant security vulnerabilities in the robot operating system.

6. Conclusions and Future Work

In this paper, we analyzed the transition from Industry 4.0 to Industry 5.0 in the context of robotic systems, with particular emphasis on collaborative robots (Cobots), the role of telecommunications operators, and the resulting security challenges. We also present an original view of the architecture of a Cobot-based system and analyze it from several architectural perspectives. In addition, we outline the potential contribution of a

telecommunications operator, and provide an original comparison of security challenges related to Cobots in the context of Industry 4.0 and Industry 5.0.

It can be highlighted that Industry 5.0 does not introduce a completely new technological foundation. Rather, it builds upon the achievements of Industry 4.0 and its underlying technologies, reusing and reorienting them towards a more human-centric, sustainable, and resilient industrial model. Technologies such as AI, machine learning, Big Data analytics, Cloud and Edge Computing, IoT, digital twins, and blockchain remain important, but their roles are changing. In Industry 5.0, they are increasingly applied to support human–machine collaboration, safety, personalization, and sustainability, rather than being used solely for automation and efficiency. Apparently, Industry 5.0 offers a promising path toward more human-oriented industrial systems, but its successful adoption will depend on ensuring trust, safety, privacy, and resilience in increasingly complex robotic environments.

The human factor becomes central. Unlike Industry 4.0, which tended to reduce direct human participation in production, Industry 5.0 emphasizes human–machine cooperation. Cobots are a representative example of this shift, as they are designed to assist workers, improve ergonomics, and adapt to human needs and contexts.

Telecommunications operators gain a broader role. Even now, operators are no longer limited to providing connectivity. They can contribute through private networks, network slicing, MEC, Cloud services, security services, and support for digital sovereignty. These capabilities make them important enablers of Industry 5.0 deployments.

Security requirements become more complex. While many threats resemble those already known from Industry 4.0, Industry 5.0 increases the impact of these risks due to the close interaction between humans, robots, AI systems, and sensitive data. New concerns include biometric privacy, spoofing, deepfakes, AI model poisoning, physical safety risks, and ethical compliance.

Cobots create both opportunities and risks. They can improve productivity, flexibility, and worker support, but they also significantly increase the attack surface. In particular, the combination of increased human influence, shared workspaces for humans and machines, dynamic decision-making, and AI-based behavior requires stronger protection mechanisms than in traditional industrial automation. It requires that Verticals, industrial automation vendors, independent software vendors, Cloud service providers, and telecommunications operators work out a way to share responsibility along the liability chain.

Security must be considered from a broader perspective. In Industry 5.0, cybersecurity is no longer only a technical issue. It also includes physical safety, while the importance of trust, privacy, compliance, and organizational resilience is amplified. In such a case, security management is more interdisciplinary and more closely connected to human-centered design. In particular, it is important to identify the stakeholders responsible for eliminating or minimizing the risks associated with specific security threats and challenges, and to define the relevant security procedures.

This paper has identified several research topics and gaps related to the implementation of Cobots in Industry 5.0 environments supported by telecommunications operators. Addressing these gaps and exploring the identified research topics will require further investigation in the following key areas:

- Defining and testing concrete protection mechanisms for Cobots. They include methods for securing control channels, sensor data, AI models, and human–machine interfaces.
- Developing telecom-operator security frameworks for Industry 5.0. An important question is how operators can provide secure and trustworthy environments and services for Cobot ecosystems, including private networks, MEC, slicing, and AI services. Future solutions should take advantage of the capabilities of the 6G network,

as well as integrate AI solutions and security and privacy protection systems belonging to the telecommunications operator and Industry 5.0.

- Studying attack detection and response in human–robot environments. More work is needed on detecting deepfakes, spoofing, model manipulation, and abnormal robot behavior in real time.
- Improving privacy-preserving processing of human data. Since Industry 5.0 systems may collect biometric, behavioral, and contextual data, future solutions should reduce exposure while still enabling useful analytics.
- Strengthening resilience and fail-safe behavior. Especially in the Cobot area, research is needed on graceful degradation, recovery procedures, and robust fallback strategies when network or AI services degrade or become unavailable. A proper framework is needed for mission-critical services delivered by Cobots, designed to operate under the constraints of the CAP theorem.
- Assessing ethical and regulatory implications. As Cobots and AI systems become more integrated into workplaces and interact with workers, future efforts should address legal compliance, explainability of actions, and accountability.

Author Contributions: Conceptualization, T.W.N., K.B. and J.-P.W.; methodology, T.W.N., M.S., Z.K., T.P., A.P., K.B. and J.-P.W.; validation, T.P., A.P. and K.B.; formal analysis, T.P., A.P., K.B. and J.-P.W.; investigation, T.W.N., M.S., Z.K., T.P., A.P., K.B. and J.-P.W.; resources, T.W.N., M.S. and Z.K.; visualization, T.W.N., M.S. and Z.K.; writing—original draft preparation, T.W.N., M.S., Z.K. and T.P.; writing—review and editing, T.W.N., M.S. and Z.K.; supervision, Z.K., K.B. and J.-P.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: Authors Tomasz Pawlikowski, Aleksandra Podlasek, Krzysztof Bocianiak are employed by the company Orange Polska. Author Jean-Philippe Wary is employed by the company Orange Innovation, France. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth-Generation Mobile Network
6G	Sixth-Generation Mobile Network
ACID	Atomicity, Consistency, Isolation, Durability
AI	Artificial Intelligence
API	Application Programming Interface
APN	Access Point Name
AR	Augmented Reality
BASE	Basic Availability, Soft State, Eventual Consistency
BCI	Brain–Computer Interface
CAP	Consistency, Availability, Partition Tolerance
CDN	Content Delivery Network
Cobot	Collaborative Robot
CPS	Cyber-Physical System
CTI	Cyber Threat Intelligence
EE	Essential Entities
EEG	Electroencephalography

eMBB	enhanced Mobile Broadband
ERP	Enterprise Resource Planning
eSIM	Embedded SIM
GDPR	General Data Protection Regulation
gNB	Next-Generation NodeB
ICT	Information and Communications Technology
IE	Important Entities
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
LTE-M	Long Term Evolution for Machines
MEC	Multi-access Edge Computing
ML	Machine Learning
mMTC	Massive Machine Type Communication
MR	Mixed Reality
NB-IoT	NarrowBand Internet of Things
NIS2	Network and Information Systems Directive 2
NTN	Non-Terrestrial Networks
OT	Operational Technology
PLMN	Public Land Mobile Network
PPE	Personal Protective Equipment
PTP	Precision Time Protocol
ROS	Robot Operating System
SCADA	Supervisory Control and Data Acquisition
SCM	Supply Chain Management
SIM	Subscriber Identity Module
SLA	Service Level Agreement
S-NSSAI	Single-Network Slice Selection Assistance Information
SOC	Security Operations Center
TO	Telecommunications Operator
TSN	Time-Sensitive Networking
URLLC	Ultra-Reliable and Low-Latency Communication
VR	Virtual Reality
Wi Fi	Wireless Fidelity
XaaS	Everything-as-a-Service
XR	Extended Reality

References

1. Noble, S.M.; Mende, M.; Grewal, D.; Parasuraman, A. The Fifth Industrial Revolution: How Harmonious Human–Machine Collaboration is Triggering a Retail and Service [R]evolution. *J. Retail.* **2022**, *98*, 199–208. [\[CrossRef\]](#)
2. Szabó-Szentgróti, G.; Végvári, B.; Varga, J. Impact of Industry 4.0 and Digitization on Labor Market for 2030-Verification of Keynes’ Prediction. *Sustainability* **2021**, *13*, 7703. [\[CrossRef\]](#)
3. Dieste, M.; Orzes, G.; Culot, G.; Sartor, M.; Nassimbeni, G. The “dark side” of Industry 4.0: How can technology be made more sustainable? *Int. J. Oper. Prod. Manag.* **2024**, *44*, 900–933. [\[CrossRef\]](#)
4. Enang, E.; Bashiri, M.; Jarvis, D. Exploring the transition from techno centric industry 4.0 towards value centric industry 5.0: A systematic literature review. *Int. J. Prod. Res.* **2023**, *61*, 7866–7902. [\[CrossRef\]](#)
5. Ghobakhloo, M.; Mahdiraji, H.A.; Iranmanesh, M.; Jafari-Sadeghi, V. From Industry 4.0 Digital Manufacturing to Industry 5.0 Digital Society: A Roadmap Toward Human-Centric, Sustainable, and Resilient Production. *Inf. Syst. Front.* **2024**. [\[CrossRef\]](#)
6. Zorzenon, R.; Lizarelli, F.L.; de Moura, D.B.A.A. What is the potential impact of industry 4.0 on health and safety at work? *Saf. Sci.* **2022**, *153*, 105802. [\[CrossRef\]](#)
7. Badri, A.; Boudreau-Trudel, B.; Souissi, A.S. Occupational health and safety in the industry 4.0 era: A cause for major concern? *Saf. Sci.* **2018**, *109*, 403–411. [\[CrossRef\]](#)
8. Nahavandi, S. Industry 5.0—A Human-Centric Solution. *Sustainability* **2019**, *11*, 4371. [\[CrossRef\]](#)

9. Coelho, P.; Bessaa, C.; Landeck, J.; Silvaa, C. Industry 5.0: The Arising of a Concept. *Procedia Comput. Sci.* **2023**, *217*, 1137–1144. [\[CrossRef\]](#)
10. Alves, J.; Lima, T.M.; Gaspar, P.D. Is Industry 5.0 a Human-Centred Approach? A Systematic Review. *Processes* **2023**, *11*, 193. [\[CrossRef\]](#)
11. Rajkumar, N.; Nachiappan, B.; Mathews, A.; Radha, V.; Viji, C.; Kovilpillai, J.A. Industry 5.0: The human-centric future of manufacturing. In *Challenges in Information, Communication and Computing Technology*; CRC Press: Boca Raton, FL, USA, 2024. [\[CrossRef\]](#)
12. Graziani, A.R.; Cantini, G.; Pini, F.; Dell’Amico, M.; Vergnano, A. A Shift Toward Industry 5.0: A Practical Assessment Framework for Human-Centric, Sustainable, and Resilient Industry. *Sustainability* **2026**, *18*, 6330. [\[CrossRef\]](#)
13. Gilbert, S.; Lynch, N. Brewer’s conjecture and the feasibility of consistent, available, partition-tolerant web services. *ACM SIGACT News* **2002**, *33*, 51–59. [\[CrossRef\]](#)
14. Shabur, M.; Shahriar, A.; Ara, M.A. From automation to collaboration: Exploring the impact of Industry 5.0 on sustainable manufacturing. *Discov. Sustain.* **2025**, *6*, 341. [\[CrossRef\]](#)
15. Martini, B.; Bellisario, D.; Coletti, P. Human-Centered and Sustainable Artificial Intelligence in Industry 5.0: Challenges and Perspectives. *Sustainability* **2024**, *16*, 5448. [\[CrossRef\]](#)
16. Khan, S.; Liu, X.; Arshad Ali, S.; Alam, M. Storage Solutions for Big Data Systems: A Qualitative Study and Comparison. *arXiv* **2019**, arXiv:1904.11498. [\[CrossRef\]](#)
17. Niewolski, W.; Nowak, T.W.; Sepczuk, M.; Kotulski, Z.; Artych, R.; Bocianiak, K.; Wary, J.-P. Security Context Migration in MEC: Challenges and Use Cases. *Electronics* **2022**, *11*, 3512. [\[CrossRef\]](#)
18. Zeb, S.; Mahmood, A.; Khowaja, S.A.; Dev, K.; Hassan, S.A.; Gidlund, M.; Bellavista, P. Towards defining industry 5.0 vision with intelligent and softwarized wireless network architectures and services: A survey. *J. Netw. Comput. Appl.* **2024**, *223*, 103796. [\[CrossRef\]](#)
19. Ravi, D.K.; Chavhan, S. Shift to 6G: Exploration on trends, vision, requirements, technologies, research, and standardization efforts. *Sustain. Energy Technol. Assess.* **2022**, *54*, 102666. [\[CrossRef\]](#)
20. Calvanese Strinati, E.; Barbarossa, S. 6G networks: Beyond Shannon towards semantic and goal-oriented communications. *Comput. Netw.* **2021**, *190*, 107930. [\[CrossRef\]](#)
21. Leng, J.; Guo, J.; Xie, J.; Zhou, X.; Liu, A.; Gu, X.; Mourtzis, D.; Qi, Q.; Liu, Q.; Shen, W.; et al. Review of manufacturing system design in the interplay of Industry 4.0 and Industry 5.0 (Part II): Design processes and enablers. *J. Manuf. Syst.* **2025**, *79*, 528–562. [\[CrossRef\]](#)
22. Leng, J.; Guo, J.; Xie, J.; Zhou, X.; Liu, A.; Gu, X.; Mourtzis, D.; Qi, Q.; Liu, Q.; Shen, W.; et al. Review of manufacturing system design in the interplay of Industry 4.0 and Industry 5.0 (Part I): Design thinking and modeling methods. *J. Manuf. Syst.* **2024**, *76*, 158–187. [\[CrossRef\]](#)
23. Lessi, C.C.; Gavrielides, A.; Solina, V.; Qiu, R.; Nicoletti, L.; Li, D. 5G and Beyond 5G Technologies Enabling Industry 5.0: Network Applications for Robotics. *Procedia Comput. Sci.* **2024**, *232*, 675–687. [\[CrossRef\]](#)
24. Mahmood, A.; Abedin, S.F.; Sauter, T.; Gidlund, M.; Landernäs, K. Factory 5G: A Review of Industry-Centric Features and Deployment Options. *IEEE Ind. Electron. Mag.* **2022**, *16*, 24–34. [\[CrossRef\]](#)
25. Wang, Z.; Yan, H.; Wang, Y.; Xu, Z.; Wang, Z.; Wu, Z. Research on Autonomous Robots Navigation based on Reinforcement Learning. In *Proceedings of the 2024 3rd International Conference on Robotics, Artificial Intelligence and Intelligent Control (RAIIC), Mianyang, China, 5–7 July 2024*; IEEE: New York, NY, USA, 2024; pp. 78–81. [\[CrossRef\]](#)
26. Rejeb, A.; Rejeb, K.; Zrelli, I.; Kayikci, K.; Hassoun, A. The research landscape of Industry 5.0: A scientific mapping based on bibliometric and topic modeling techniques. *Flex. Serv. Manuf. J.* **2025**, *37*, 1203–1250. [\[CrossRef\]](#)
27. Zafar, M.H.; Falkenberg Langås, E.; Sanfilippo, F. Exploring the synergies between collaborative robotics, digital twins, augmentation, and industry 5.0 for smart manufacturing: A state-of-the-art review. *Robot. Comput.-Integr. Manuf.* **2024**, *89*, 102769. [\[CrossRef\]](#)
28. Islam, M.T.; Sepanloo, K.; Woo, S.; Woo, S.H.; Son, Y.-J. A Review of the Industry 4.0 to 5.0 Transition: Exploring the Intersection, Challenges, and Opportunities of Technology and Human–Machine Collaboration. *Machines* **2025**, *13*, 267. [\[CrossRef\]](#)
29. Valette, E.; El-Haouzi, H.B.; Demesure, G. Industry 5.0 and its technologies: A systematic literature review upon the human place into IoT- and CPS-based industrial systems. *Comput. Ind. Eng.* **2023**, *184*, 109426. [\[CrossRef\]](#)
30. AIOTI WG Standardisation. IoT and Edge Computing Impact on Beyond 5G: Enabling Technologies and Challenges, Release 3.0. 30 November 2023. Available online: <https://aioti.eu/wp-content/uploads/2023/11/AIOTI-Report-IoT-and-Edge-impact-on-Beyond-5G-R3-Final.pdf> (accessed on 28 January 2026).
31. Rejeb, A.; Rejeb, K.; Keogh, J.G.; Süle, E. When Industry 5.0 Meets the Circular Economy: A Systematic Literature Review. *Circ. Econ. Sust.* **2025**, *5*, 2621–2652. [\[CrossRef\]](#)

32. Ghobakhloo, M.; Iranmanesh, M.; Fathi, M.; Rejeb, A.; Foroughi, B.; Nikbin, D. Beyond Industry 4.0: A systematic review of Industry 5.0 technologies and implications for social, environmental and economic sustainability. *Asia-Pac. J. Bus. Adm.* **2025**, *17*, 889–914. [\[CrossRef\]](#)
33. Castillo, C.; Otero-Romero, T.; Alvarez-Palau, E.J. Navigating the transition to industry 5.0: Advancing sustainability, resilience, and human-centricity in Spanish supply chain management. *Discov. Sustain.* **2025**, *6*, 331. [\[CrossRef\]](#)
34. Pérez-Lara, M.; Saucedo-Martínez, J.A.; Marmolejo-Saucedo, J.A.; Salais-Fierro, T.E.; Vasant, P. Vertical and horizontal integration systems in Industry 4.0. *Wirel. Netw.* **2020**, *26*, 4767–4775. [\[CrossRef\]](#)
35. Sharma, R. Industry 5.0: A Balancing Act—Efficiency, Ethics, and the Human Factor. Available online: <https://www.linkedin.com/pulse/industry-50-balancing-act-efficiency-ethics-human-factor-sharma-ejb1c> (accessed on 28 January 2026).
36. Shah, M.; Monapara, P.; Chitroda, Y.; Karetiya, D.; Patel, D. Investment Casting Using Additive Manufacturing: State-of-the-Art and Future Directions—A Review Paper. In *Proceedings of the 2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC)*, Rajkot, India, 2023; IEEE: New York, NY, USA, 2024; pp. 889–895. [\[CrossRef\]](#)
37. Sala, D.; Richert, M. Perspectives of Additive Manufacturing in 5.0 Industry. *Materials* **2025**, *18*, 429. [\[CrossRef\]](#) [\[PubMed\]](#)
38. Xiang, W.; Yu, K.; Han, F.; Fang, L.; He, D.; Han, Q.-L. Advanced Manufacturing in Industry 5.0: A Survey of Key Enabling Technologies and Future Trends. *IEEE Trans. Ind. Inform.* **2024**, *20*, 1055–1068. [\[CrossRef\]](#)
39. Angulo, C.; Chacón, A.; Ponsa, P. Towards a cognitive assistant supporting human operators in the Artificial Intelligence of Things. *Internet Things* **2023**, *21*, 100673. [\[CrossRef\]](#)
40. Meini, V.; Bachi, L.; Omezzine, M.A.; Prociassi, G.; Pigni, F.; Billeci, L. Artificial Intelligence for the Analysis of Biometric Data from Wearables in Education: A Systematic Review. *Sensors* **2025**, *25*, 7042. [\[CrossRef\]](#) [\[PubMed\]](#)
41. Singh, S.K.; Sengupta, S. Sovereign AI: Rethinking Autonomy in the Age of Global Interdependence. *arXiv* **2025**, arXiv:2511.15734. [\[CrossRef\]](#)
42. Trunina, I.; Bilyk, M.; Yakovenko, Y. Artificial Intelligence from Industry 5.0 Perspective: Threats and Challenges. In *Proceedings of the 2023 IEEE 5th International Conference on Modern Electrical and Energy System (MEES)*, Kremenchuk, Ukraine, 2023; IEEE: New York, NY, USA, 2024; pp. 1–5. [\[CrossRef\]](#)
43. Urbaniak, D.; Bro Damsgaard, S.; Zhang, W.; Rosell, J.; Suárez, R.; Suppa, M. Distributed Control for Collaborative Robotic Systems Using 5G Edge Computing. *IEEE Access* **2024**, *12*, 148706–148718. [\[CrossRef\]](#)
44. 3GPP. Network Slicing Security for 5G and 5G Advanced Systems. Available online: <https://www.3gpp.org/technologies/slicing-security> (accessed on 28 January 2026).
45. Orange. 5G Campus Network. Available online: <https://www.orange.pl/duze-firmy/siec-kampusowa-5g> (accessed on 28 January 2026).
46. Kotulski, Z.; Nowak, T.; Sepczuk, M.; Bocianiak, K.; Pawlikowski, T.; Podlasek, A.; Wary, J.-P. Keeping Verticals’ Sovereignty During Application Migration in Continuum. *J. Netw. Syst. Manag.* **2024**, *32*, 67. [\[CrossRef\]](#)
47. Orozco, R.P.; Malinen, J.; Porambage, P.; Dopazo, D.A.; Muñoz, R.; Prats, P.A.; Vilalta, R.; Giardina, P.G.; De Angelis, M.; Land, G. Intent-Based Service Provisioning and Closed-Loop Automation for Cobot Service Migration in a Multi-Stakeholder Environment. *IEEE Trans. Netw. Serv. Manag.* **2025**, *22*, 4192–4205. [\[CrossRef\]](#)
48. Singh Gaba, G.; Sari, A.; Butun, I.; Singh, P.; Gurtov, A.; Liyanage, M. A Survey on Security and Privacy of Industry 4.0 and Beyond: Technical Aspects, Use Cases, Challenges, and Research Directions. *IEEE Open J. Commun. Soc.* **2025**, *6*, 8865–8929. [\[CrossRef\]](#)
49. Holfelder, W.; Mayer, A.; Baumgart, T. Sovereign cloud technologies for scalable data spaces. In *Designing Data Spaces*; Otto, B., Ten Hompel, M., Wrobel, S., Eds.; Springer: Cham, Switzerland, 2022. [\[CrossRef\]](#)
50. STACKIT. The Sovereign Cloud for Europe. Available online: <https://stackit.com/en> (accessed on 28 January 2026).
51. Poli, S. Reinforcing Europe’s Technological Sovereignty Through Trade Measures: The EU and Member States’ Shared Sovereignty. *Eur. Pap.* **2023**, *8*, 429–445. [\[CrossRef\]](#) [\[PubMed\]](#)
52. Shradha, C.S.; Aaradhana, D.A. Beyond boundaries: Quantum cryptography safeguarding industry 5.0 in smart cities. In *Proceedings of the 8th IET Smart Cities Symposium (SCS 2024)*, Hybrid Conference, Bahrain, 2024; IET: Bengaluru, India, 2025; pp. 303–308. [\[CrossRef\]](#)
53. Oliva del Moral, J.; DeMarti Iolius, A.; Vidal, G.; Crespo, P.M.; Etxezarreta Martinez, J. Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. *IEEE Internet Things J.* **2024**, *11*, 30217–30244. [\[CrossRef\]](#)
54. Ogiela, U.; Ogiela, M.R. Personalized Cryptography in Cybersecurity Systems. In *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*. 3PGCIC 2022; Lecture Notes in Networks and Systems; Barolli, L., Ed.; Springer: Cham, Switzerland, 2023; Volume 571. [\[CrossRef\]](#)
55. Tashkinov, A.G. The application of industry 4.0 into the company’s production activities through effective decision-making. *Sci. Rep.* **2025**, *15*, 34202. [\[CrossRef\]](#) [\[PubMed\]](#)
56. Rakholia, R.; Suarez-Cetrulo, A.L.; Singh, M.; Carbajo, R.S. Integrating AI and IoT for Predictive Maintenance in Industry 4.0 Manufacturing Environments: A Practical Approach. *Information* **2025**, *16*, 737. [\[CrossRef\]](#)

57. Ericsson. Opening 5G Networks to App Developers. Available online: <https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/opening-5g-networks-to-app-developers> (accessed on 28 January 2026).
58. Afrin, S.; Rafa, S.J.; Kabir, M.; Farah, T.; Bin Alam, M.S.; Lameesa, A.; Ahmed, S.F.; Gandomi, A.H. Industrial Internet of Things: Implementations, challenges, and potential solutions across various industries. *Comput. Ind.* **2025**, *170*, 104317. [CrossRef]
59. Barrett, J. 5G RedCap: Unlocking Scalable IoT and FWA Innovation with Reduced Capability 5G. 5 August 2025. Available online: <https://www.3gpp.org/news-events/partner-news/redcap-gsa-article01> (accessed on 28 January 2026).
60. Nowak, T.W.; Sepczuk, M.; Kotulski, Z.; Niewolski, W.; Artych, R.; Bocianiak, K.; Osko, T.; Wary, J.-P. Verticals in 5G MEC-Use Cases and Security Challenges. *IEEE Access* **2021**, *9*, 87251–87298. [CrossRef]
61. ElFar, O.A.; Chang, C.-K.; Leong, H.Y.; Peter, A.P.; Chew, K.W.; Show, P.L. Prospects of Industry 5.0 in algae: Customization of production and new advanced technology for clean bioenergy generation. *Energy Convers. Manag.* **2021**, *10*, 100048. [CrossRef]
62. Wang, X.; Xue, Y.; Zhang, J.; Hong, Y.; Guo, S.; Zeng, X. A Sustainable Supply Chain Design for Personalized Customization in Industry 5.0 Era. *IEEE Trans. Ind. Inform.* **2024**, *20*, 8786–8797. [CrossRef]
63. Cotta, W.A.A.; Lopes, S.I.; Vassallo, R.F. Towards the Cognitive Factory in Industry 5.0: From Concept to Implementation. *Smart Cities* **2023**, *6*, 1901–1921. [CrossRef]
64. Vernon, D. The Space of Cognitive Vision. In *Cognitive Vision Systems*; Lecture Notes in Computer Science; Christensen, H.I., Nagel, H.H., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 3948. [CrossRef]
65. Iqbal, A.; Nauman, A.; Hussain, R.; Bilal, M. Cognitive D2D communication: A comprehensive survey, research challenges, and future directions. *Internet Things* **2023**, *24*, 100961. [CrossRef]
66. Cao, H.; Söderlund, H.; Derspeisse, M.; Johansson, B. Exploring the current applications and potential of extended reality for environmental sustainability in manufacturing. *arXiv* **2023**, arXiv:2312.17595. [CrossRef]
67. Cao, H.; Söderlund, H.; Fang, Q.; Chen, S.; Erdal, L.; Gubartalla, A.; Lopes, P.V.; Shao, G.; Lonnehed, P.; Putto, H.; et al. Towards AI-based Sustainable and XR-based human-centric manufacturing: Implementation of ISO 23247 for digital twins of production systems. *arXiv* **2025**, arXiv:2508.14580. [CrossRef]
68. Sharma, M.; Tomar, A.; Hazra, A. Edge Computing for Industry 5.0: Fundamental, Applications, and Research Challenges. *IEEE Internet Things J.* **2024**, *11*, 19070–19093. [CrossRef]
69. Rüzgar, N. Human Resistance to Automation and the Fear of Job Displacement. In *Navigating Human-Machine Collaboration in Smart Factories*; Naidoo, V., Prasad Vemuri, V., Verma, R.R., Eds.; IGI Global Scientific Publishing: Hershey, PA, USA, 2026; pp. 195–212. [CrossRef]
70. Varma, A.; Vajpayee, A.; Sanghani, P. Organizational Culture of Industry 5.0: Exploration Analysis in Multinational and National Companies. In *Proceedings of the 2024 International Conference on Intelligent and Innovative Practices in Engineering and Management (IIPEM), Singapore, 25 November 2024*; IEEE: New York, NY, USA, 2025; pp. 1–6. [CrossRef]
71. Fraga-Lamas, P.; Fernández-Caramés, T.M.; Rosado da Cruz, A.M.; Lopes, S.I. An Overview of Blockchain for Industry 5.0: Towards Human-Centric, Sustainable and Resilient Applications. *IEEE Access* **2024**, *12*, 116162–116201. [CrossRef]
72. Amazon News. AWS Bahrain Region Disrupted by Ongoing Conflict. Available online: <https://www.aboutamazon.com/news/aws-bahrain-region-middle-east-conflict> (accessed on 7 April 2026).
73. Ahmed, Z.; Kakarla, J.H.H.; Hazra, A.; Gurusamy, M. Quantum machine learning for industry 5.0: Fundamental, applications and research challenges. *Comput. Sci. Rev.* **2026**, *61*, 100976. [CrossRef]
74. Salawu, G.; Glen, B. Quantum Computing as a Disruptive Technology: Implications for Advanced Manufacturing and Industry 5.0. *Appl. Sci.* **2026**, *16*, 4856. [CrossRef]
75. Fournier, É.; Jeoffrion, C.; Hmedan, B.; Pellier, D.; Fiorino, H.; Landry, A. Human-Cobot collaboration's impact on success, time completion, errors, workload, gestures and acceptability during an assembly task. *Appl. Ergon.* **2024**, *119*, 104306. [CrossRef] [PubMed]
76. OpenBCI Homepage. Available online: <https://openbci.com/about> (accessed on 22 November 2025).
77. Sun, T.; Yu, Y.; Zheng, Q.; Wang, Z.; Zheng, C. Extended reality: Enhancing human-centered capabilities for human-cyber-physical systems (HCPS). *Procedia CIRP* **2024**, *130*, 368–373. [CrossRef]
78. The Sedona Conference. U.S. Biometric Systems, Privacy Primer. *Sedona Conf. J.* **2024**, *25*, 163. Available online: <https://www.thesedonaconference.org/sites/default/files/publications/Biometric-Systems-Privacy-Primer-May-2024.pdf> (accessed on 3 June 2026).
79. Tu, X. Industrial Metaverse: Revolutionizing Industry 5.0 with Digital Twins and Extended Reality. Ph.D. Thesis, Department of Mechanical Engineering, Aalto University, Espoo, Finland, 2024.
80. Kwon, W.; Yang, J.; Song, S.; Lee, J.; Kim, H. Real-Time Digital-Twin-Based Cobot-Worker Collision Risk Prediction Using Unity, ROS, and UWB. *IEEE Access* **2025**, *13*, 85967–85978. [CrossRef]
81. Ford, N.; Richards, M.; Sadalage, P.; Dehghani, Z. *Software Architecture: The Hard Parts: Modern Trade-Off Analyses for Distributed Architectures*; O'Reilly Media: Sebastopol, CA, USA, 2021; ISBN 978-1492086895.

82. Shaping Europe's Digital Future. Uses of Radio Spectrum. Available online: <https://digital-strategy.ec.europa.eu/en/policies/uses-radio-spectrum> (accessed on 16 May 2026).
83. Shaping Europe's Digital Future. Radio Spectrum CEPT Mandates. European Commission. 11 November 2014. Available online: <https://digital-strategy.ec.europa.eu/en/library/radio-spectrum-cept-mandates> (accessed on 16 May 2026).
84. Shaping Europe's Digital Future. France: 3.8–4.2 GHz Spectrum Opened for Industrial 5G Private Networks. European Commission. 22 December 2025. Available online: <https://digital-strategy.ec.europa.eu/en/miscellaneous/france-38-42-ghz-spectrum-opened-industrial-5g-private-networks> (accessed on 16 May 2026).
85. Shaping Europe's Digital Future. Poland: Regulator Consults on 3.8–4.2 GHz Spectrum for Private 5G Networks. European Commission. 26 November 2025. Available online: <https://digital-strategy.ec.europa.eu/en/miscellaneous/poland-regulator-consults-38-42-ghz-spectrum-private-5g-networks> (accessed on 16 May 2026).
86. 5G Spectrum for Local Industrial Networks. Leveraging Communications Service Provider Assets and Expertise, Ericsson White Paper GFTL ER 20:003151. March 2025. Available online: <https://www.ericsson.com/en/reports-and-papers/white-papers/5g-spectrum-for-local-industrial-networks> (accessed on 16 May 2026).
87. GSMA, 5G Advanced. Available online: <https://www.gsma.com/solutions-and-impact/technologies/networks/5g-network-technologies-and-solutions/5g-advanced/> (accessed on 28 January 2026).
88. ETSI. Multi-Access Edge Computing (MEC). Available online: <https://www.etsi.org/technologies/multi-access-edge-computing> (accessed on 28 January 2026).
89. TS 33.501; Security Architecture and Procedures for 5G System. 3GPP: Valbonne, France, 2018. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169> (accessed on 28 January 2026).
90. TS 23.003; Numbering, Addressing and Identification. 3rd Generation Partnership Project. Technical Specification Group Core Network and Terminals. V19.6.0 (2026-03) Release 19. 3GPP: Valbonne, France, 2026. Available online: https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/19.06.00_60/ts_123003v190600p.pdf (accessed on 28 January 2026).
91. Onopa, S.; Kotulski, Z. State-of-the-Art and New Challenges in 5G Networks with Blockchain Technology. *Electronics* **2024**, *13*, 974. [CrossRef]
92. Sieć 5G w Łódzkiej Specjalnej Strefie Ekonomicznej. Available online: <https://www.orange.pl/duze-firmy/Lodzka-Specjalna-Strefa-Ekonomiczna> (accessed on 15 June 2026).
93. Sieć Kampusowa 5G w Fabryce Przyszłości. Available online: <https://www.orange.pl/duze-firmy/miele> (accessed on 15 June 2026).
94. G Arrives in Le Havre: Optimised Communications and a Smart Port on the Horizon. Available online: <https://hellofuture.orange.com/en/5g-arrives-in-le-havre-optimised-communications-and-a-smart-port-on-the-horizon/> (accessed on 15 June 2026).
95. IEEE 1588-2019; IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. IEEE SA: Piscataway, NJ, USA, 2020. Available online: <https://standards.ieee.org/ieee/1588/6825/> (accessed on 28 January 2026).
96. ISO 50001; Energy Management. ISO: Geneva, Switzerland. Available online: <https://www.iso.org/iso-50001-energy-management.html> (accessed on 28 January 2026).
97. Tomaszewski, L.; Kołakowski, R. Mobile Services for Smart Agriculture and Forestry, Biodiversity Monitoring, and Water Management: Challenges for 5G/6G Networks. *Telecom* **2023**, *4*, 67–99. [CrossRef]
98. Magedanz, T.; Corici, M.I. Getting ready for 6G Research—Understanding Technological Drivers towards 6G and Emerging 6G Management Requirements. In *Tutorial at IEEE/IFIP NOMS, 25 April 2022*; Fraunhofer FOKUS: Berlin, Germany, 2022. Available online: <https://noms2022.ieee-noms.org/program/tutorials> (accessed on 3 June 2026).
99. Tariq, F.; Khandaker, M.R.A.; Wong, K.-K.; Imran, M.A.; Bennis, M.; Debbah, M. A Speculative Study on 6G. *IEEE Wirel. Commun.* **2020**, *27*, 118–125. [CrossRef]
100. Rajatheva, N.; Atzeni, I.; Bjornson, E.; Bourdoux, A.; Buzzi, S.; Dore, J.B.; Erkucuk, S.; Fuentes, M.; Guan, K.; Hu, Y.; et al. White Paper on Broadband Connectivity in 6G. *arXiv* **2020**, arXiv:2004.14247. [CrossRef]
101. ENISA. Cybersecurity of Critical Sectors. Advancing Cybersecurity and Resilience of the Union's Critical Infrastructure. Available online: <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors> (accessed on 28 January 2026).
102. Abishek, B.A.; Kavyashree, T.; Jayalakshmi, R.; Tharunkumar, S.; Raffik, R. Collaborative Robots and Cyber Security in Industry 5.0. In *Proceedings of the 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 16–17 June 2023*; IEEE: New York, NY, USA, 2023; pp. 1–6. [CrossRef]
103. Santos, B.; Costa, R.L.C.; Santos, L. Cybersecurity in Industry 5.0: Open Challenges and Future Directions. In *Proceedings of the 2024 21st Annual International Conference on Privacy, Security and Trust (PST), Sydney, Australia, 28–30 August 2024*; IEEE: New York, NY, USA, 2024; pp. 1–6. [CrossRef]

104. Arputharaj, J.V.; Sandeep, J.; Prasad, D.D.; Adu-Manu, K.S. Navigating Data Privacy in Industry 5.0: Advanced Strategies for Sustainability. In *Soft Computing in Industry 5.0 for Sustainability*; Reddy, C.K.K., Sithole, T., Ouaisa, M., Ozer, O., Hanafiah, M.M., Eds.; Springer: Cham, Switzerland, 2024. [[CrossRef](#)]
105. Flores Gonzalez, J.M.; Coronado, E.; Yamanobe, N. ROS-Compatible Robotics Simulators for Industry 4.0 and Industry 5.0: A Systematic Review of Trends and Technologies. *Appl. Sci.* **2025**, *15*, 8637. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.