

# Systematic Analysis of Risks in Industry 5.0 Architecture

Muhammad Ali Hassan <sup>1</sup>, Shehnila Zardari <sup>2,\*</sup>, Muhammad Umer Farooq <sup>1</sup>, Marwah M. Alansari <sup>3,\*</sup> and Shima A. Nagro <sup>3,\*</sup>

<sup>1</sup> Department of Computer Science and Information Technology, NED University of Engineering and Technology, Karachi 75270, Pakistan; mohammadalihassan06@gmail.com (M.A.H.); umer@neduet.edu.pk (M.U.F.)

<sup>2</sup> Department of Software Engineering, NED University of Engineering and Technology, Karachi 75270, Pakistan

<sup>3</sup> College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia

\* Correspondence: shehniraz@cloud.neduet.edu.pk (S.Z.); m.alansari@seu.edu.sa (M.M.A.); s.nagro@seu.edu.sa (S.A.N.)

**Abstract:** Industry 4.0, which was proposed ten years ago to address both the industry's strengths and faults, has finally been replaced by Industry 5.0. It seeks to put human welfare at the core of manufacturing systems, achieving societal goals beyond employment and growth to firmly provide wealth for the long-term advancement of all of humanity. The purpose of this research is to examine the risks involved in the adoption of Industry 5.0's architecture. The paper discusses the significance of Industry 5.0 and the advanced technology needed for this industrial revolution, followed by a detailed discussion of Industry 5.0's human-centric strategy. The comprehensive literature review has resulted in the identification of risks and their mitigation strategies in Industry 5.0 architecture. A taxonomy with respect to different categories of risks has also been proposed. This study classifies Industry 5.0 system assets, identifies platform-independent risks, and develops countermeasures to protect against potential threats, irrespective of the business or domain.

**Keywords:** Industry 4.0; Industry 5.0; cyber security; IIoT; cobot; AI; DoS



**Citation:** Hassan, M.A.; Zardari, S.; Farooq, M.U.; Alansari, M.M.; Nagro, S.A. Systematic Analysis of Risks in Industry 5.0 Architecture. *Appl. Sci.* **2024**, *14*, 1466. <https://doi.org/10.3390/app14041466>

Academic Editors: Dimitris Mourtzis, Slavko Rakic, Ugljesa Marjanovic and Nenad Medic

Received: 23 October 2023

Revised: 6 February 2024

Accepted: 8 February 2024

Published: 11 February 2024



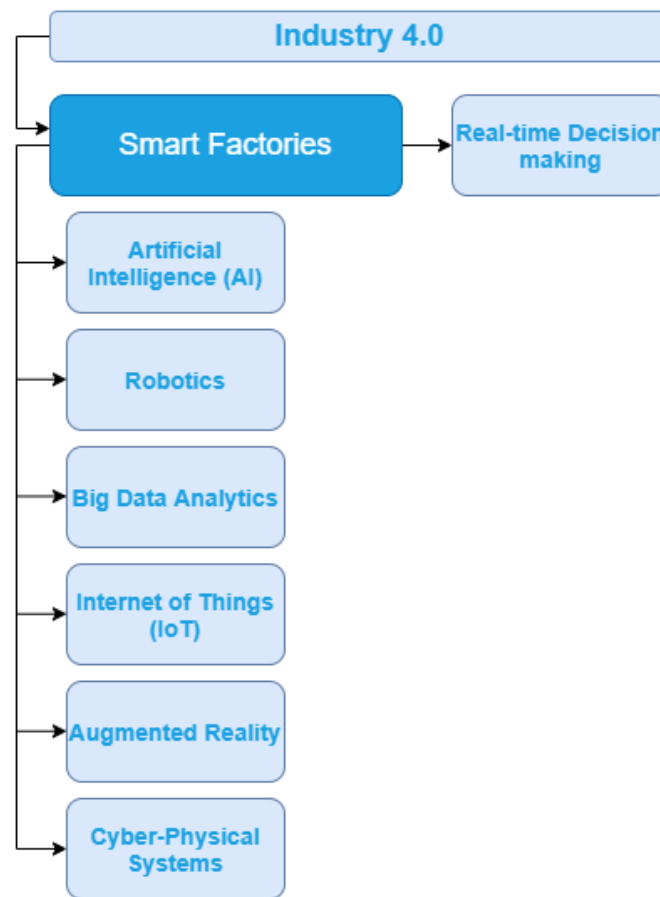
**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The current technological revolution will profoundly change the way individuals throughout the world live, work, think, and cooperate [1]. Digital technology built on artificial intelligence can handle business problems. They are utilized to achieve mass customization and enhanced production with less human work. Industry 5.0 was first proposed in 2015, but its effects on production have just begun becoming apparent. Here, cutting-edge production techniques are used to meet customized customer requests. Artificial intelligence is being used as a new tool in industrial processes to improve accuracy and performance [2].

### 1.1. Industry 4.0 Overview

Industry 4.0, the fourth industrial revolution which is strongly tied to the Internet of Things (IoT), cloud computing, big data analytics, and other technologies as mentioned in Figure 1, was developed around the concept of smart factories, i.e., a manufacturing unit where different process are linked vertically and horizontally [3]. The concept of smart factories, which is the key element in Industry 4.0, focuses on the utilization of artificial intelligence (AI), IoT, and robotics to enhance productivity, optimization, efficiency, and quality of operations. Machines are interconnected with each other to communicate with a central control system, which ensures real-time monitoring and decision-making in the smart factories of Industry 4.0 [4].



**Figure 1.** Industry 4.0 architecture [3].

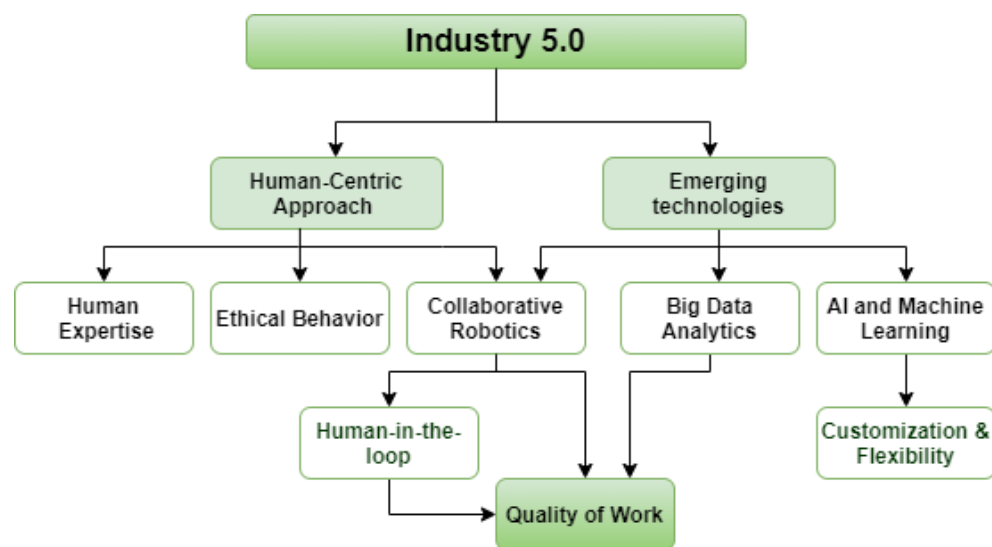
### 1.2. Industry 5.0 Overview

The issue for manufacturers throughout the world is to boost productivity while keeping people informed in the manufacturing process. This endeavor becomes increasingly challenging when emerging technologies like brain–machine interfaces and advancements in AI make robots more essential to the production process. The upcoming industrial revolution, known as Industry 5.0, can handle these problems. In a nutshell, the phrase “Industry 5.0” alludes to humans and robots cooperating rather than competing [5]. Industry 5.0 merely focuses on the workers’ knowledge, skills, and abilities, which can be incorporated with the machines [6]. It has been examined how Industry 5.0 is currently performing in relation to related research developments. Notably, supply chains, AI, big data, digital transformation, machine learning, and the Internet of Things are still key factors influencing Industry 5.0. These are the same forces that formed Industry 4.0 [7].

The three key determinants of Industry 5.0’s development are identified as human-centric, sustainable, and resilient development [8]. The term “human touch” in Industry 5.0 refers to the integration of human expertise, intelligence, and creativity with the machine to increase the effectiveness of the industrial output [9,10]. To have a better understanding of this “human touch” in Industry 5.0, consider the example of mobile manufacturing, in which machines are responsible for creating and integrating parts of mobile phones, and humans customize them according to the needs of the customer. Figure 2 illustrates how Industry 5.0’s architecture combines human and machine collaboration [7]. A different perspective characterizes Industry 5.0 as being faster, more scalable, and involving more people than earlier due to the type of technology available. This can be achieved by pushing for more sophisticated robot-human interfaces that combine human intelligence and creativity with better automation and integration of robots. Increased productivity will result from this. Industry 5.0 offers significant benefits such as increased productivity,

agility, profitability, adaptability, change-readiness, and cost reduction. By emphasizing usability, accessibility, and user experience, human-centric design principles improve security measures by guaranteeing that security protocols are simple to understand and smoothly incorporated into workflow procedures. By incorporating human-centric design concepts into security measures, organizations can cultivate a security-aware culture among staff members, enabling them to take an active role in protecting assets and reducing possible risks in Industry 5.0 environments. However, it also offers core benefits such as the evolving global society, fostering open-minded employees, and waste prevention for sustainability, cost savings, environmental protection, and better social interaction. Through the reduction of wasted materials and resources, the four types of waste prevention viewpoints have a substantial impact on both the environment and the economy. With the goal of minimizing material costs and social repercussions, these views encompass physical waste, urban waste, process waste, and social waste [11].

Acknowledging the paradigm shift from a techno-centric Industry 4.0 to a human-centric approach in intelligent and automated factories draws attention to the growing ethical issues across various industrial sectors. Ethical issues emphasize the importance of tools like Value Sensitive Design (VSD) in converting complex cultural values into practical design necessities, particularly in the context of human–machine symbiosis in the Factory of the Future [12].



**Figure 2.** Industry 5.0 architecture [7].

Along with human centrality, Industry 5.0 distinguishes itself by thoughtfully incorporating sustainable and resilient practices into the constantly changing realm of modern industrial systems, as depicted in Figure 3. To complement the evolution of Industry 4.0, Industry 5.0 represents a strategic change towards tackling socio-environmental challenges stemming from the ongoing digital industrial transition [13]. Industry 5.0, which positions itself as a comprehensive approach that fully incorporates digitalization into processes throughout organizations and supply chains, essentially aims to achieve a symbiosis of technological, social, and ecological elements. The change from a solely technological focus to one that takes into account the advantages and comfort of individuals further reinforces the sustainability element and fits in with the overall wellbeing of society in what is sometimes referred to as “Society 5.0” [14]. The circular economy is a key focus in the context of electric vehicles, emphasizing the circularity of resources in supply chains. Product-Service Systems (PSS) enable new business models for this economy. Industry 5.0’s sustainable value networks prioritize service integration and digital technologies to enhance ties between participants [15]. Global automakers prioritize sustainability through recycling and product reuse, leading to supply chain reorganization. Electric vehicles and digitization are

transforming the sector, fostering stronger supplier-manufacturer relationships through digital technology and product-related services [16].

In Industry 5.0, where complex industrial processes are vulnerable to disruptions due to the use of modern technologies like AI, big data analytics, and IoT, resilience is essential. The idea goes beyond only enduring difficulties; it also emphasizes performance enhancement and flexibility in the face of setbacks. The need for resilience has been highlighted by the COVID-19 pandemic, which implies that organizations must develop systems that can withstand disruptions and quickly bounce back. Resilience is mostly attributed to flexibility and inherent redundancy, which allow systems to overcome malfunctions or failures. To prevent and successfully respond to disruptions in the Industry 5.0 scenario, organizations need to proactively strengthen resilience through techniques like modular production systems, flexible manufacturing system designs, and risk management procedures, including cybersecurity measures [17,18]. The emphasis on resilience and sustainability is not just a catchphrase in Industry 5.0; it is a core design principle. The awareness of the essential role that humans play in this technology environment is what distinguishes Industry 5.0. A special synergy is produced when humans and machines work together. Humans are adaptable, skilled at addressing problems, and capable of making subtle decisions. This human-machine collaboration promotes sustainable operations by lowering the need for ongoing maintenance and guaranteeing steady production. Because human workers can swiftly adjust to changing circumstances and manage unforeseen problems, Industry 5.0 places a strong emphasis on the human touch as a means of developing resilience. In Industry 5.0, a holistic strategy that leverages the capabilities of both humans and robots emerges as essential to attaining sustainability and resilience.



**Figure 3.** Industry 5.0 [13].

### 1.3. Concept of Industry 5.0

Industry 4.0 was found to be less concerned with people and more with technology, dismissing the role of people in productive systems. As a result, Industry 5.0 has emerged as a complementary and transitional philosophy from a technological Industry 4.0 to a human-centered Industry 5.0, where worker wellbeing is prioritized while preserving productive performance. Moving beyond a profit-centric approach, Industry 5.0 emphasizes sustainability through a dedication to social, environmental, and societal factors. Though it emphasizes workplace safety, human-machine connections, and larger social and environmental responsibilities, the notion acknowledges the power of technology for industrial development while also tying commercial aims and social goals together. Harness in human-machine collaboration, enhancing interaction in complex industrial systems, and empowering people and operators through individual capabilities and skills are all examples of future possibilities for human centrality [19]. Based on the concepts of

the 6 R's policy of industrial recycling, Industry 5.0 may be the first to be human-driven in terms of sustainability: Recognize, Rethink, Realize, Reduce, Reuse, and Recycle waste where possible while producing/creating customized, high-quality products. However, there is still a debate about the concept of Industry 5.0, specifically how this strategy might help sustainable development [13].

Humans manage personalization and critical thinking while machines handle monotonous jobs in Industry 5.0, which integrates humans and technologies as collaborative robots [20]. Industry 5.0 is a symmetric innovation aimed at securing outputs by isolating automated systems, preparing the next generation of global governance [13,19,20].

The creation of the Digital Twin (DT), which depicts a high-fidelity, virtual, physical entity with real-time communication, is a particular aspect of using robots. [19,21]. These Industry 5.0-identified DT (Digital Twin) systems enable production optimization while conducting operational safety assessments in conjunction with simulation systems [22]. DTs, primarily focused on connectivity and production system modeling, can reduce educational inequality by promoting tele-operability and interactive robot production systems for instruction and learning [19,21,23].

#### *1.4. Difference between Industry 4.0 and Industry 5.0*

Industry 4.0 focuses on utilizing cognitive computing to integrate cloud servers with intelligent facilities and the Internet of Things in manufacturing plants, while Industry 5.0 stresses the importance of bringing human hands and brains back into the industrial setting. The eras of humans and machines are attempting to collaborate to maximize efficiency and responsible resource usage. Factory data in Industry 4.0 is collected and stored in the cloud for analysis by various instruments and sensors. Access to these data is crucial for artificial intelligence to improve goods and enhance the manufacturing environment. With the aid of intelligent manufacturing and tools like the Internet of Things, artificial intelligence, physical cyber systems, cloud computing, and cognitive computing, Industry 4.0 put a strong emphasis on customization. The human connection with production, which is made possible by increased human interaction and engagement in the production system, is one of the key components of Industry 5.0. In this revolution, applying critical thinking abilities increases the automated system's speed and precision. Industry 5.0 automates equipment updates, modernizes production systems, avoids overproduction, and selects appropriate instruments through intelligent systems. The goal of this revolution is to use digital equipment with human intelligence to speed up manufacturing and prevent errors in systems [11].

Industry 5.0 prioritizes human centricity, sustainability, and resilience, requiring logistics to balance societal, environmental, and economic aspects. Industry 4.0's smart logistics revolution aims to replace human operators and increase productivity. The emphasis in Industry 5.0 is now more on the environment and human beings, with new technologies being employed to enhance human operators rather than replace them to provide more highly customized goods and services. Many logistics providers are, in this sense, going through a smart transformation of Industry 4.0; however, this smart transformation should not be impeded but rather redirected to better accomplish societal, environmental, and economic sustainability in Industry 5.0 [24].

#### *1.5. Threats and Risks Involved*

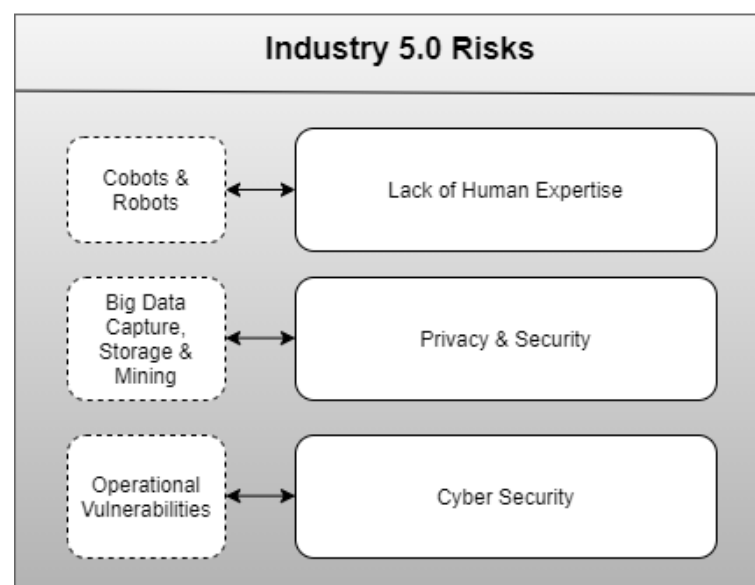
It is important to remember that the fifth industrial revolution will be fueled by cobots (collaborative robots), robots, and artificial intelligence, which will play critical roles in this sector. Despite its potential and capabilities, the industry will still require human modification and personalization skills [25].

As shown in Figure 4, most of the industries that have embraced the concepts of Industry 4.0 and Industry 5.0 are responsible for the generation of significant value through the capture, storage, and mining of big data. This has led to the creation of several opportunities in a variety of industries, including government services and even healthcare [26,27].

Given the multiple benefits that may be derived from big data, the industrial revolutions that resulted in the creation of ICT and other kinds of digital technology drove big data to become the present oil in the technological world. Because of the importance and influence of big data, organizations often spend a significant amount of money on issues related to privacy and cyber security. For instance, stricter access control restrictions must be put in place as big data are gathered and stored to guarantee that it can only be used for those purposes. However, because security and privacy issues will be treated extremely seriously, it is crucial to consider how data are shared and linked across numerous organizations and industries [25,28]. Because most industries have automated and digitalized their operations, which has revealed a variety of vulnerabilities that can substantially harm the system, cyber security in the fourth and fifth industrial revolutions has become crucial. Even though both Industries 4.0 and 5.0 are already up and running, they have brought with them several operational issues that are problematic for digital supply networks and connected smart industries [25,29].

This is because the industrial value chain may not be able to immediately mitigate the effects of a cyber-attack if one occurs. After all, those effects could be quite severe, and they are not prepared for such risks. Therefore, as Industry 4.0 transitions to Industry 5.0, addressing the cyber dangers necessitates developing robust cybersecurity strategies that must be vigilant, secure, and persistent, fully integrated into organizational and IT strategies [30]. In this discussion, cybersecurity threats in Industries 4.0 and 5.0 are evaluated. The need for maintenance and ongoing upgrades to handle these risks is highlighted [25].

The number of terminal and intermediary devices has significantly increased because of Industry 5.0's extensive adoption of IoT. Cyber threats have greater opportunities because of this increased attack surface. To safeguard infrastructure, Industry 5.0 uses blockchain-based access control systems and artificial intelligence (AI)-based intrusion detection systems (IDS). Compared to Industry 4.0, this represents a more complex and advanced approach to security. Cyber-physical systems and augmented reality (AR) are emerging supporting technologies for the Internet of Things. The harmonization of functionality may become more complex as a result of these technologies' potential introduction of new security requirements. In conclusion, Industry 5.0 highlights the use of cutting-edge technologies like blockchain and artificial intelligence for security, expands the attack surface with an emphasis on the Internet of Things, and tackles particular difficulties related to the integration of various applications and auxiliary technologies [31].



**Figure 4.** Threats and risks in Industry 5.0 [26,27].



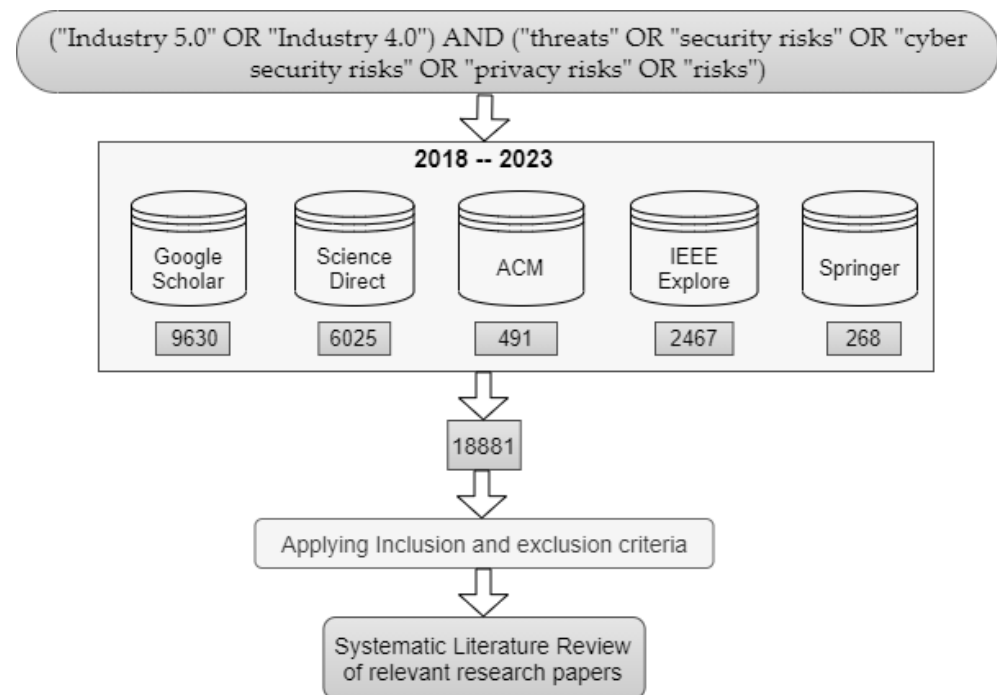
This study aims to address the following research questions by focusing on key areas to enhance understanding and provide valuable information about the topic:

- **Research Question 1:** What are the potential challenges in the adoption of Industry 5.0, considering factors like compatibility with existing systems, workforce training, and technological complexities?  
The motivation behind this research question is to address the potential issues related to the adoption of Industry 5.0, which are crucial if one is to fully profit from it. It is important to comprehend these difficulties, including compatibility with current systems, workforce training, and technological complexity, to ensure a successful and seamless transition to Industry 5.0.
- **Research Question 2:** What technologies Industry 5.0 may use for supply chain transparency and traceability have for data privacy?  
The purpose of this research question is to address issues including product safety, labor rights, and environmental sustainability. There has been a growing focus on increasing supply chain transparency and traceability. Industry 5.0 can provide a chance to accomplish these objectives.
- **Research Question 3:** What issues should be taken into account while using Industry 5.0 to enhance security, worker safety, and wellbeing?  
The goal of this research question is to investigate how Industry 5.0 might be used to enhance worker safety and wellbeing in light of increased automation and the expanding usage of robotics and AI in production.

## 2. Methodology

A systematic literature review (SLR) was carried out for this study to thoroughly evaluate pertinent papers related to Industry 4.0 and Industry 5.0, with a particular emphasis on related risks and threats. (“Industry 5.0” OR “Industry 4.0” AND “threats” OR “security risks” OR “cybersecurity risks” OR “privacy risks” OR “risks”) was the search query used to find relevant research publications. The academic works published as journal articles, conference papers, or book chapters between 2018 and 2023 were included in the inclusion criteria. To include the most current and pertinent contributions to the subject, the review’s scope was restricted to this time frame. In contrast, studies not directly relevant to Industry 5.0 and 4.0 or not addressing the risks and threats associated with them were filtered out using exclusion criteria. Moreover, research not written in English and those whose whole texts were unavailable were not included. The advantage of this SLR is that it offers a thorough understanding of the state of the art when it comes to the threats and risks related to Industry 5.0. This helps practitioners, researchers, and decision-makers to improve cybersecurity and minimize possible risks in the changing industrial landscape.

As depicted in Figure 5, SLR methodology was used in this study to analyze papers that were found in several significant databases, including IEEE Xplore, Google Scholar, Science Direct, ACM, and Springer. The original dataset included many publications: a total of 18881 papers from all databases, including 9630 from Google Scholar, 6025 from Science Direct, 491 from ACM, 2467 from Springer, and 268 from IEEE Xplore. Strict inclusion and exclusion criteria, as previously mentioned, were utilized to guarantee a targeted and pertinent review. As shown in Figure 6, a selected group of studies surfaced after these criteria were applied, and these papers served as the foundation for the systematic literature review. This methodical approach sought to extract important insights from the large body of literature, adding to a thorough knowledge of the field of study.



**Figure 5.** Systematic Literature Review Methodology.



**Figure 6.** Number of publications after inclusion/exclusion criteria over 2018–2023.

### 3. Literature Review

The results of a thorough analysis of research publications related to the topic are presented in Tables 1–4 below. The key factors of this study include all the risks identified with its affected assets, risk mitigation strategies (if any), and all the challenges. This technique addresses all the risks, threats, and challenges that Industry 5.0 has been facing. All the advantages and disadvantages of Industry 5.0 are then discussed. With the help of this literature review, practitioners and researchers will be able to see a comprehensive list of risks in Industry 5.0. This will help the practitioners who are trying to adopt Industry 5.0 to make informed choices about such a transition.



**Table 1.** Identified Cybersecurity Risks in Industry 5.0.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[9]	Trust risk: there are significant risks because of AI and automation, and there is a need to build trust in ecosystems.	ICT (Information and Communications Technology) systems, Data	The deployment of IoT nodes using “Authentication” and “trusted security” as a security mechanism when interacting with diverse devices.	Establishing security and trust in ecosystems.
[32]	The possibility of cyber-physical vulnerabilities resulting from the integration of cyberspace and physical space in Human-cyber-physical systems (HCPS) raises the possibility of compromised decision-making processes, data breaches, and system malfunctions.	cyber-physical systems, data confidentiality, and security	To protect data and system integrity, mitigation techniques may involve putting strong cybersecurity measures in place, such as intrusion detection systems, access limits, and encryption.	Some of the challenges that may arise are making sure that cyber and physical components are compatible and interoperable, addressing privacy issues regarding the collecting and use of personal data in HCPS, and encouraging stakeholders to trust and accept automated decision-making processes.
[33]	Smart contracts enhance security in decentralized asset management (DAM), but their irreversible nature poses risks, as hackers can use faults to steal tokens, posing a threat to blockchain transactions.	Integrity and security of financial assets, data saved and exchanged on blockchain networks.	Adopt secure coding standards, code audits, and testing for smart contract vulnerabilities, incorporating encryption and multi-factor authentication to protect private information and prevent illegal transactions.	Smart contract transactions are irreversible, making it challenging to identify and correct mistakes or fraudulent activity and retrieve lost or stolen money due to security breaches or malicious activity.
[34]	Data privacy risks in healthcare, particularly IoT-based systems, pose a significant challenge in supply chain management, particularly in managing data privacy and integration.	Data, supply chain, planning cycles	Industry 5.0 utilizes decentralized IIOT (Industrial Internet of Things), blockchain middleware, and mass customization to integrate data in smart manufacturing from numerous sources and services.	One of the key challenges faced by the shipping sector is data privacy.
[35,36]	Eavesdropping, intercepting, or hijacking: Unauthorized access or management of sensitive data	IIoT communication channels, network setup	Implement secure communication protocols and encryption	Protecting wireless networks and avoiding “man-in-the-middle” attacks
[35]	Brute force attacks: Constant and repeated efforts to guess passwords or keys	IIoT end devices, servers, and applications	Implement secure password guidelines and account lockout features.	Security and usability must be balanced, and access credentials must be managed.
[35]	Denial of Service: Interruption of processes and potential physical threats	IIoT end devices, Industrial Control Systems	Network segmentation and intrusion detection systems implementation	Timely component and configuration vulnerability analysis
[37]	Security risks include adversarial AI, the responsibility gap, and the unpredictable nature of industrial AI-based systems.	Industrial AI systems, critical industrial assets	ML (Machine-Learning) algorithms should be improved and tested against adversarial AI.	Costly failures and changes, price of skill, high standards for regulations, legal and regulatory difficulties.

Table 1. Cont.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[38]	Privacy issues may include compromised data integrity and confidentiality, unauthorized access and theft of node identities	IIoT devices, data	Implement encryption, secure authentication, and access control measures.	Limited autonomy, a lack of computational resources, and efficient access control mechanisms.
[38]	Data exposure, data integrity difficulties, confidentiality issues, DoS (Denial of Service) attacks, and authentication challenges	Cloud/Fog services, data, Big data repositories, Virtualized resources.	Implement reliable monitoring, encryption, and access control procedures.	Challenging to detect fraudulent behavior, lack of trust in service providers, and lack of control over access policies.
[39]	Malicious reconfiguration of sensors	Sensors, manufacturing information architecture	Put security measures in place to stop unauthorized sensor reconfiguration.	Systems of the next generation do not prioritize security.
[39]	Security flaws being exploited by attack vectors.	Industrial manufacturing equipment, manufacturing information architecture	Regularly update software and firmware, create firewalls and network segments, and evaluate the security situation in industrial equipment design.	Problems with security implementation's compatibility. Security of networked systems is difficult.
[39]	Compromise of platforms and infrastructure	Computers used for Computer-aided Design (CAD) design, industrial network domain	Put strong cybersecurity safeguards in place for CAD design machines. Apply security patches and software updates on a regular basis. Implement strict access and authentication controls.	The widespread use of cloud-based architecture creates new security difficulties. Providing uniform security measures across platforms and infrastructure can be challenging.
[40]	Cybersecurity threats like direct and indirect attacks on service providers' IT systems.	Industrial networks, transportation systems, and manufacturing-related items and equipment with connectivity.	The process of improving industrial control systems' cybersecurity resilience involves system identification, vulnerability analysis, stakeholder involvement, NIST Framework, DevOps approach, improved attack tree, risk evaluation methods, and STRIDE security analysis.	The importance of cyber security in industrial systems is crucial for Industry 4.0 management, and enhancing industrial management support is vital for comprehensive studies.
[41]	Cyber espionage: Industry 4.0 is exposed to cyber espionage due to smart and linked corporate operations. Industry 4.0 has become a favorite target for well-organized cybercriminal gangs looking to steal intellectual property and sensitive data.	Virtual data, violation of commercial agreements, industrial control systems.	Technologies for intrusion detection and prevention and security evaluation, and industrial control systems (ICS) risk management, software updates, secure communication	Integrity protection, layered encryption.

Table 1. Cont.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[41]	DoS attacks are common in factories due to interdependent equipment and the importance of the unavailability of certain devices in the production environment.	Cloud services, servers.	Encryption of data streams, access control/multiple authorization.	These attacks are unpredictable and difficult to handle.
[42]	Industry 4.0 businesses face significant cybersecurity risks due to the increased interconnectivity of smart devices, sensors, and actuators, including Industrial Control Systems and IIoT gateways.	Data integrity, data confidentiality and data availability, productive time, violation of commercial agreements.	The DevOps approach enhances industrial security, visualizes security risks using an attack tree, assesses risks in smart manufacturing systems using a hierarchical model, and calculates IoT cyber risk economic impacts.	Modern industrial equipment with smart devices and wireless networks or wired Ethernet can create potential entry points for cyberattacks due to the lack of proper design for cybersecurity.
[43]	Small and Medium-Sized Enterprises (SMEs) face cybersecurity risks due to weak supply chain links and lack of awareness in Industry 4.0, resulting in inconsistent measurements of supply chain cyber risks.	Recovery planning in the supply chains of Small and Medium-Sized Enterprises.	SMEs must invest a sizable amount of money in cyber security and recovery planning; cyber risk puts them at a disadvantage.	In all the examined Industry 4.0 technical advancements, there is a lack of clarity regarding disaster recovery plans.
[44]	Computational load for IoT devices, blockchain implementation, and security risks in IoT	IoT devices like sensors.	Implement a blockchain-based IoT framework to stop different attacks and use machine learning to lighten the computational load on IoT devices.	Blockchain communication protocols may cause data corruption, while IoT devices may face high computational burden due to machine-learning solutions, impacting their functionality and usage.
[45]	Loss of intellectual property and security of the data.	Data, intellectual property	Implementation of data security measures.	Protection of sensitive information.
[46]	The study predicts an increase in future cyberattacks on AI projects, particularly in medical devices and data, necessitating a robust cybersecurity strategy.	Medical devices and data	To ensure sustainable and scalable AI projects, it is crucial to have a robust security architecture, educate staff on security measures, and foster trust within the project environment.	Analyze the medical device industry's awareness of security issues and the approaches used to address them.
[47]	Cyber-attack.	Information systems, infrastructures, computer networks, and personal electronic devices.	The Industrial Process System Environment Strategy uses the Cyber Risk Analysis in the Industrial Process (CRISP) approach to evaluate how cyberattacks will affect specific devices or the system as a whole.	To effectively implement the CRISP approach, access to process documentation and the Asset Management System is crucial for risk assessment.

**Table 1.** *Cont.*

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[48]	Cybersecurity risk, implementation cost, lack of financial resources, lack of skilled workers.	Data, human resources, businesses.	N/A	Resistance of employees to change.
[49]	Cybersecurity risks due to inadequate infrastructure in Industry 4.0	Machines and data	N/A	By connecting devices to the Internet without taking adequate security precautions, unauthorized users can access the devices remotely and cause damage.

**Table 2.** Identified Workforce and Training Risks in Industry 5.0.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[36,50,51]	Human resource risk: It will be difficult to find workers with the specialized skills required for the new procedures in Industry 4.0, which also calls for better pay.	Human capital and employee engagement.	Universities and educational institutions must ensure that study programs are updated because Industry 4.0 is made up of many different technologies. This will ensure that there are enough people available to execute Industry 4.0.	Train labor to work with robots and machines.
[52]	Industry 5.0 demands multidisciplinary and multi-technical knowledge, increasing demand for well-trained workers.	Efficiency and effectiveness of training programs.	N/A	Training becomes challenging, especially in sustainable development goals emphasizing lifelong learning for future worker development.
[51]	Lack of understanding of the circumstances and activities taking place on the shop floor.	Shop floor personnel, machine statuses, order progress.	Enable real-time monitoring and improve data visibility.	Training and awareness, data security and privacy
[34]	Human resource risk: To work in such an atmosphere, the staff need sufficient training. To enable these smart workers to work in the manufacturers' smart environments, strong management practices are needed.	Human capital and employee engagement.	Industry 5.0 is built on effective communication between humans and robots with a focus on human centricity.	Train labor to work with robots and machines. Predictive maintenance of machines required.

Table 2. Cont.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[9]	Skills gap and training challenges: To effectively collaborate with advanced robots and smart machines, human workers must have competency skills.	Human workers	N/A	Adoption of advanced technology, training, and skill development.
[53]	Industry 4.0 adoption may face workforce and technological challenges, including digital skills shortages, competency gaps, employee wellbeing concerns, and cybersecurity threats.	Workforce wellbeing and safety, data.	Workforce training and up skilling.	The implementation of worker wellbeing monitoring technologies, particularly among the aging workforce and persons with impairments. There is a dearth of skilled employees with digital capabilities.
[49]	Adaptation of skills: The days of standard employment profiles are over. Workers in Industry 4.0 must adapt to jobs and abilities that are outside the scope of their current responsibilities.	Employee, organization, human resources.	N/A	Such demands may put staff under excessive strain and may reduce support for Industry 4.0 techniques.
[44]	Technology and workforce challenges	Technology, workforce	N/A	Industry 4.0 implementation may pose challenges to worker safety and productivity due to inadequate digital skills training and competency gaps.

Table 3. Identified Operational and Implementation Risks in Industry 5.0.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[34]	Technical integration: Producing low-quality products can result from the use of technologies that are not capable of coping with digitalization.	Low-quality products.	Industry 5.0 promotes human centricity, blending creativity with machine accuracy and deploying robots for repetitive tasks to increase productivity and enhance product quality.	New IT (Information Technology) technology installation calls for more effort.

Table 3. Cont.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[54]	To keep risks at a manageable level, risk management entails risk identification, assessment, and mitigation.	Objectives of the organization, a range of objectives, options for the organization, and risk management options.	Risk management involves identifying, assessing, and reducing potential hazards through systematic strategies, comparing alternatives, and following cycles for creating, planning, assessing, and deciding on acceptable risks.	Ensuring that risk management is integrated into general management; understanding the permitted ranges and risk characteristics; recording and sharing results to aid in making decisions; ensuring the efficacy and acceptability of the solutions selected
[37]	Operational risks and challenges: High talent costs, high regulatory constraints, and high costs of failure and change.	Human resources, existing investments.	Demonstrate compelling Return On Investment (ROI), Enhance recruitment and retention strategies.	Costs associated with change and failure, competing for the best talent, prerequisites for adhering to compliance requirements are crucial challenges in the realm of industrial AI.
[53]	Organizations' inadequate readiness for Industry 4.0, including inadequate planning for new supply models and smart technologies, may hinder the realization of benefits during the transitional period.	Organization	Implementing smart safety technologies, integration of self-learning machines, and adoption of cobots.	Organizations are lagging in readiness for Industry 4.0, with only 20% of new supply models and 15% of smart and autonomous technologies considered ready.
[44]	Poor readiness of Industry 4.0.	Industry 4.0's implementation.	N/A	Insufficient planning for new supply models and smart technologies could cause transitory phase issues and hinder the realization of their benefits.
[44]	Implementation and complexity problems, insufficient justification, and lack of understanding	ML for cyber security, intelligent factory integration.	The integration of blockchain and machine-learning technology in intelligent manufacturing requires technical expertise and careful configuration, as machine-learning results can be challenging to interpret and comprehend.	Organizations struggle with designing and integrating blockchain and machine-learning technologies for enhanced security due to complexity, requiring clear explanations and vision for effective training and security analysis.
[55]	Barriers to the implementation of Industry 4.0	Industry 4.0's implementation	The task involves a comprehensive analysis of all factors influencing Industry 4.0 adoption, considering inter-dependencies.	Concerns about data security, a competent workforce, workplace disputes, a lack of financial resources, and a lack of digital readiness.
[51]	Supply chain disruption.	Supply chain operations.	Supply chain diversification and risk analysis should be used.	Keeping a global supply chain's complexity and cooperation under control.



**Table 3.** *Cont.*

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[55]	Companies in both developed and developing countries lack digital readiness.	Small and medium-sized companies.	Gain more understanding of Industry 4.0, concentrate on strategic rather than purely financial issues, and handle organizational opposition.	Lack of awareness of Industry 4.0's strategic importance, organizational resistance on the part of workers, and middle management levels.
[49]	Failure of machines: cascade machine failures, which occur when one machine failure leads to another, and significant costs associated with enhancing machine security.	Machines	N/A	N/A

**Table 4.** Identified Other Risks in Industry 5.0.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[51]	Fragmented system landscape and difficulties in system integration	IT Systems.	Create standards for system interoperability and use integration frameworks.	Compatibility with legacy systems, technical difficulty.
[9]	Investments are needed to adopt cutting-edge technology like cobots in Industry 5.0, covering the costs of technology acquisition and human workforce training.	Human resources, company finances	N/A	Financial and cost management
[36]	Connectivity risk: In Industry 4.0, technology is heavily reliant on machinery.	Network connection and communication channels.	It is imperative to identify and address any new, unique machinery demands as soon as feasible.	Utilize sensing techniques for data collection, learning, and automated decision-making, ensuring components can be tracked throughout the value chain for each created item.

Table 4. Cont.

Ref. Study	Risks Identified	Assets Affected	Risk Mitigation Strategies	Challenges
[36]	Educational risks: Industry 4.0's new developments could lead to increased inequality and societal splintering, as well as the loss of numerous jobs.	Learning and development.	Universities and educational institutions must ensure that study programs are updated because Industry 4.0 is made up of many different technologies. This will ensure that there are enough people available to execute Industry 4.0.	Industry 4.0 implementations demand specialized knowledge in numerous technology fields.
[56]	Adverse learning and dependency risk involves the development of bad habits and poor decisions due to machines learning in good faith, leading to increased reliance on machines, potentially causing harm.	Workforce and organizational resilience.	The Human–Machine Cooperation (HMC) approach is a model involving cooperative agents, humans and machines, working together to achieve common goals and manage interferences to modify their decisions and actions.	N/A
[51]	Existing manual processes are costly and prone to mistakes.	Labor-intensive processes, production systems.	Automation and robotics implementation, improved process documentation.	The initial investment in automation and resistance to change.
[37]	Technical risks or challenges include those related to training, testing costs and complexity, huge state spaces, and data storage and collection.	Industrial AI systems, data storage and acquisition infrastructure.	Enhance preprocessing methods and data quality and employ high-fidelity simulations.	Cost and complexity of data acquisition, limited labeled training data, testing disruption, complexity of industrial systems.
[57]	Safety and security risks in human-robot collaboration.	Workers' mental health, robots, collaborative workspace, industrial process, control systems.	Calculate the degree of injuries caused by collision. Reduce injury in interactions between humans and robots. Prevent crashes and accidental contact.	Understanding human limits and pain tolerance is crucial for developing safe, effective human-robot collaboration systems in Industry 4.0, requiring effective mechanical systems and collision detection procedures.
[45]	Limited access to technology	Technology	N/A	Unclear cost–benefit analysis, high investment levels.
[46]	Businesses need to efficiently handle data for scalable AI solutions, requiring a strong data environment to handle large volumes of computational demands.	Data-intensive AI projects.	Cost–benefit analysis.	High cost and investments.

#### 4. Outcomes of the Studies

Following the completion of the systematic literature review, it is evident from Figure 7, which represents Table 5 that the risks related to Industry 4.0 and Industry 5.0 may be divided into three main categories: cybersecurity risk, operational and implementation risk, and workforce and training risk. Although there are more risk categories, these three are the most common. Knowing these three key risk categories is essential to moving the discussion along.



**Figure 7.** Frequency of identified risks based on Table 5.

**Table 5.** Types of risks present in reference studies.

Risks	Reference Studies
Workforce and training risk	[9,34,36,44,48–53]
Financial and investment risk	[9,46,48]
Security risk	[9,37]
Cybersecurity risk	[32–36,38–49,55]
Operational and implementation risk	[34,35,37,43,44,49,51,53–55,57]
Technological risk	[36,45,56]
Social and societal risk	[36]
System integration risk	[34,51]
Information and Knowledge Gap Risk	[51]
Technical risk	[37]
Information security risk	[38,45]

##### 4.1. Cybersecurity Risks

Over the past few years, interest in cyber security has significantly increased. As our world becomes increasingly connected, real-time system availability is becoming increasingly important. As a result, enterprises must pay close attention to maintaining and preserving their information assets to prevent the effects that cyberattacks may have on them. The assets play a big role in critical corporate operations. Additionally, users and customers are increasingly appreciating the value of the information provided by various

technologies. A cybersecurity risk is the result of the likelihood that a cybersecurity-related incident will occur and its possible effects. It includes a variety of hazards with different technology, attack routes, and techniques, but they all have two things in common: they might have a big impact, and people might think that they are improbable. To identify and manage these dangers, which were previously viewed as unlikely and hence received little attention, cyber security entails activities. Due to their unpredictable nature and the requirement for specialized ways to detect and classify them, cybersecurity risks require a different strategy for management than other categories of hazards [58].

Confidentiality, integrity, and availability are the three main security objectives as shown in Figure 8, and in a cybersecurity attack, these objectives are violated, leading to attacks on digital systems, networks, and data. It considers the potential for unauthorized access, data breaches, system outages, and data theft.



**Figure 8.** Principles of cyber security [34].

#### 4.2. Operational and Implementation Risks

The difficulties and unknowns that organizations encounter when implementing new technology or procedures are referred to as operational and implementation risks. The practical ramifications of introducing new systems, practices, or strategies within an organization are tied to these risks. They can result from several things, including human errors, technical difficulties, poor planning, and opposition to change.

Operational risk is the potential for a loss brought on by either outside events or insufficient or poor internal processes, people, or systems [59].

Contrarily, implementation risks concentrate on the difficulties and barriers that appear when implementing new technology or procedures. These hazards could include issues with adjusting to new systems, a lack of personnel training and knowledge, and insufficient funding or resources for implementation.

#### 4.3. Workforce and Training Risks

Risks related to the workforce's capacity and readiness for utilizing new technology or processes are referred to as workforce and training risks. Particularly in the context of technical breakthroughs and digital revolutions like Industry 4.0, these risks are concentrated around the human resource component of adopting new projects. On the other hand, training hazards might include insufficient training programs, resistance to training, the cost of training, etc., in the workforce, which could include a shortage of competent workers, a competency gap, a generational difference, etc. Risks related to the workforce and training must be effectively addressed if new technologies are to be successfully implemented and used.

### 5. Discussion

The goal of the systematic literature review (SLR) carried out for this study was to explore and analyze the risks, threats, and challenges related to Industry 5.0 and its related fields. We have learned important things about the new risks and weaknesses in a variety of fields, such as data security, health, education, the environment, business, and mixed domains, through a thorough study of pertinent research studies as mentioned in Table 6 above. The results of the SLR are interpreted and analyzed in this discussion, with a focus on their implications for a more comprehensive understanding of risks in the context of Industry 5.0. This study's taxonomy as shown in Figure 9 above, in contrast to Industry 4.0, is primarily concerned with human-machine collaboration since, with humans returning to the game, there are greater risks involved in their training and adoption of new technology according to Figure 10.

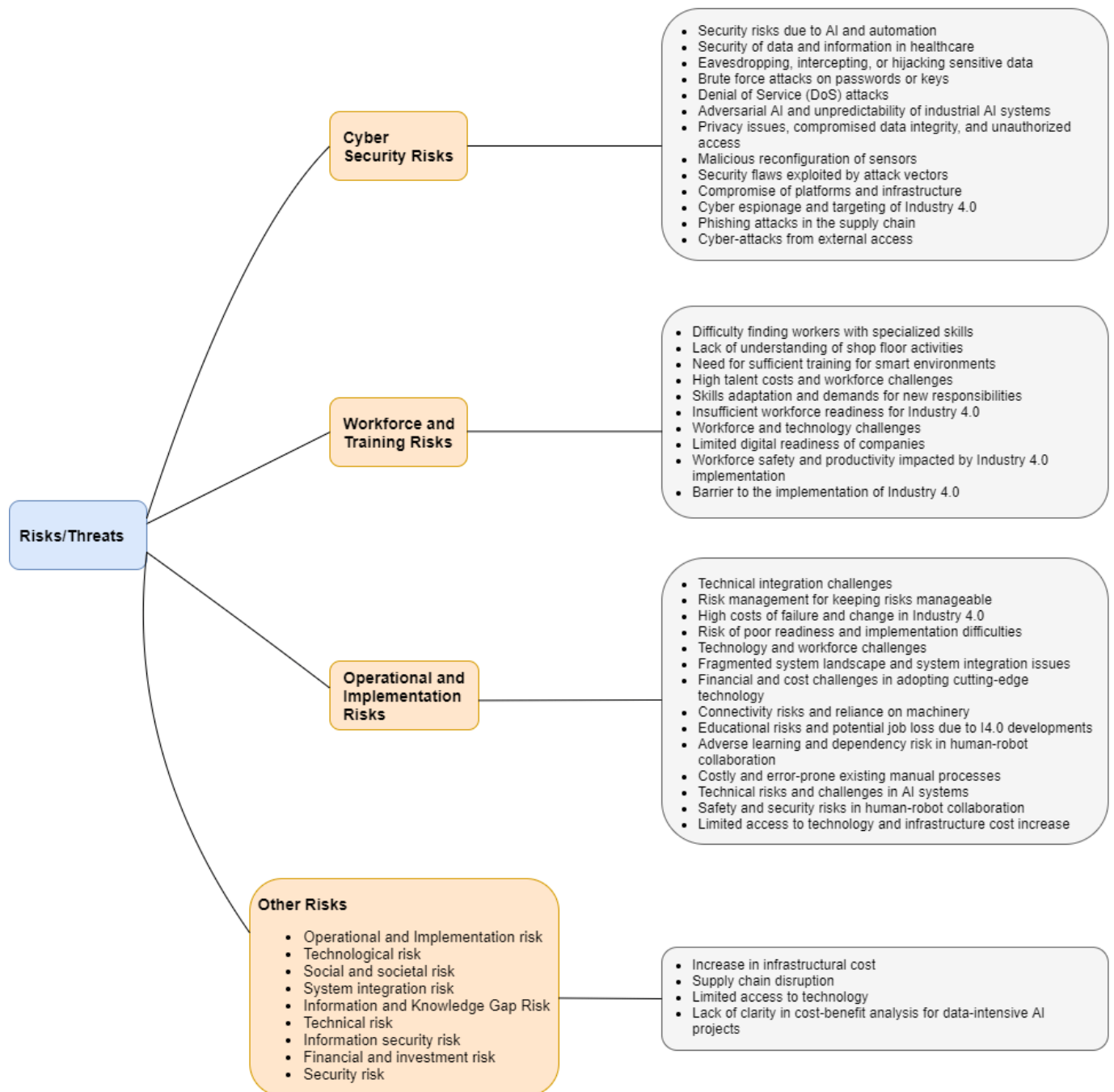
**Table 6.** Risk Classification Based on Domains.

Domains	Reference Studies
Data Security	[9,32–49]
Health	[46]
Education	[34,36,50,51]
Environment	No related references.
Business	[51–53,55]
Mixed domains	[51,54,56,57]

The concept of “Industry 5.0” is still being discussed and studied and is not yet extensively used [52]. In comparison to Industry 4.0, Industry 5.0 is still in an early stage, and there may still be questions regarding what it really involves and how it varies from Industry 4.0. It still has not attained the same degree of acceptance and recognition as Industry 4.0. Due to Industry 4.0's maturity and established principles, the body of research that is now available focuses mostly on it. There is a lack of comprehensive literature about Industry 5.0, and it has been difficult to locate relevant publications that are only concerned with this new idea. This paper's focus is on the risks discovered within the framework of Industry 4.0 to ensure a thorough review of risks and obstacles. IoT presents challenges in developing nations, especially in finding high-quality hardware, sensors, and devices for IoT 4.0 and 5.0 implementation. High costs and a lack of qualified individuals hinder industrial adoption of IoT and automation despite potential cost reductions. Manufacturing facilities that employ IoT in conjunction with blockchain technology to protect their privacy and security will have to deal with significant upfront expenditures and ongoing problems to build a block of transactions. Attacks on Internet of Things systems emphasize the necessity of thorough security designs, which include effective cryptography research and safe systems [24].

Industry 5.0's digital infrastructure is at risk from cyberattacks, posing risks to unauthorized access, data breaches, and industrial processes. Physical security threats, such as unauthorized access or equipment tampering, can also impact digital assets. Supply chain

disruptions due to natural disasters or geopolitical crises can cause critical component shortages, affecting production and financial losses. Industry 5.0 systems need robust supply chain plans, physical security, and cybersecurity measures to mitigate risks [31].



**Figure 9.** Taxonomy of major risks present in Industry 4.0 and Industry 5.0.

According to what has been observed so far, Industry 4.0 presents one of the biggest challenges for cyber security because it relies on IoT, cloud computing, AI, and other technologies that make systems and data vulnerable to attacks from malicious individuals. In light of this, Industry 5.0 also utilized these technologies, and cybersecurity threats are enormous. Unauthorized access to robots, the alteration of AI algorithms, or the interruption of human–machine communication are all examples of cybersecurity hazards. Strong cybersecurity measures, including encryption, access control, secure communication proto-



cols, intrusion detection systems, and routine software updates, are required by Industry 4.0 and Industry 5.0 to handle these concerns. To keep one step ahead of cyber attackers, organizations also need to engage in employee training to raise security awareness and regularly monitor and assess their systems for any vulnerabilities. Overall, cyber security continues to be a crucial component of Industry 4.0 and Industry 5.0, and it is crucial to adequately handle these risks to guarantee the safe and secure adoption of cutting-edge technology in the industrial sphere. Security is a barrier since Industry 5.0 must be established before ecosystem trust can be built. When deploying IoT nodes, authentication is used to interface with a variety of devices and protect against future quantum computing applications. The use of automation and AI in Industry 5.0 presents difficulties for the business and calls for trustworthy security. Since ICT systems are at the core of Industry 5.0 applications, strict security standards are required to avoid security risks. Risks associated with Industry 5.0's integration of cyber-physical systems (CPS) include supply chain vulnerabilities, cybersecurity threats, privacy concerns, operational safety, interoperability issues, and ethical problems. Robust encryption, redundancy, fault-tolerant design, and ethical concerns are only a few of the components of an all-encompassing strategy that must be based on technological, regulatory, and ethical considerations to guarantee secure CPS integration. Because of the diversity of the technical landscape, Industry 5.0 presents varying risks connected with different types of assets. Safety issues are raised by robotics, necessitating careful programming and tangible fail-safes to stop mishaps. AI systems provide ethical and privacy challenges that necessitate open algorithms and compliance with data protection laws. The introduction of cybersecurity vulnerabilities by IoT devices highlights the necessity of secure communication methods and frequent updates to minimize the risk of possible breaches. To meet the particular problems of each asset class, which include ethical, regulatory, and technical aspects, customized risk management solutions are needed [60].

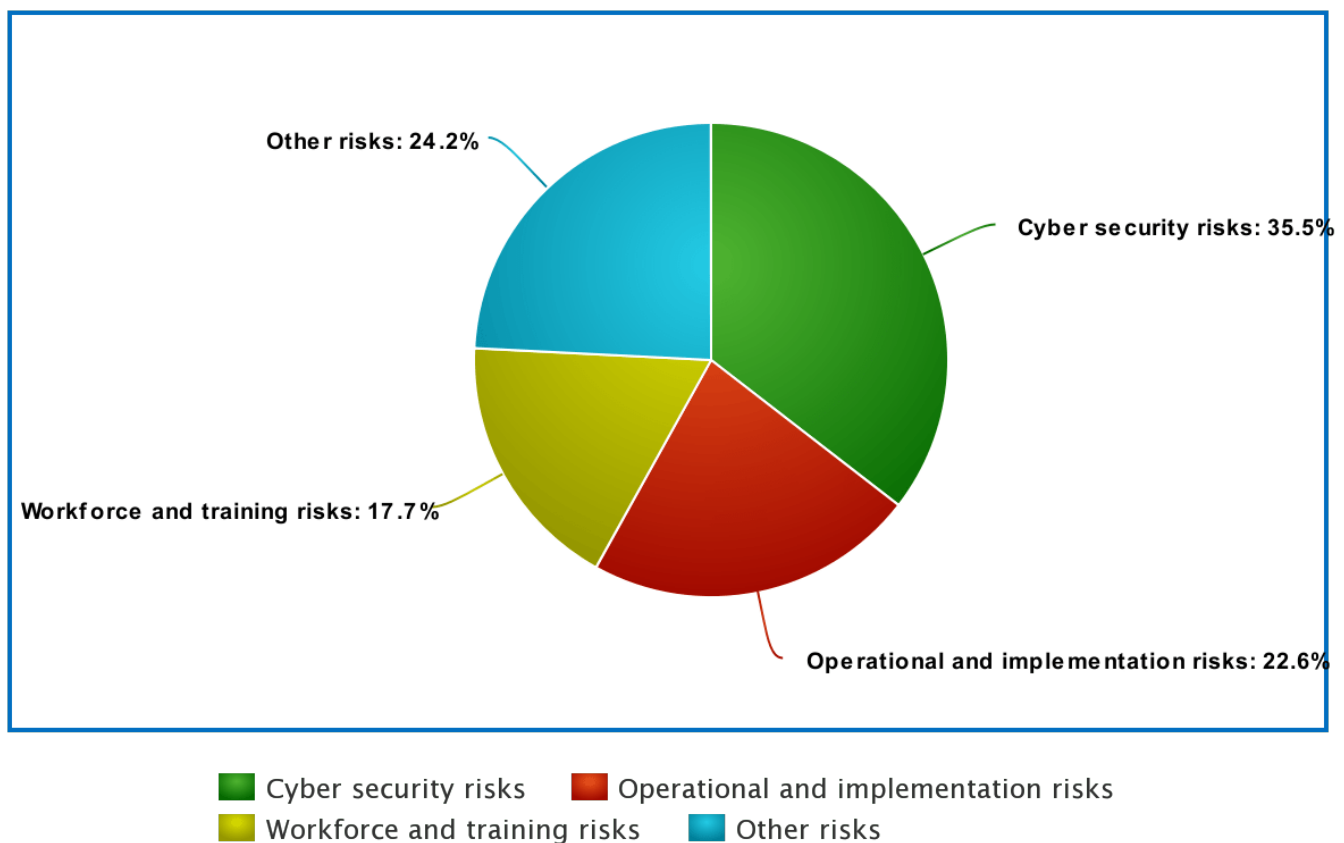


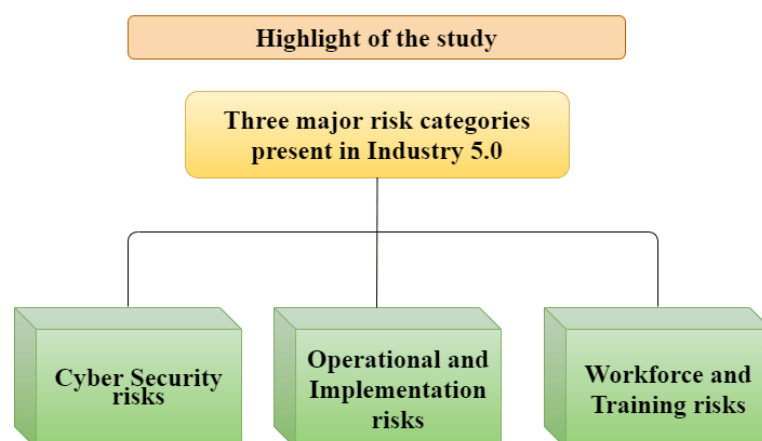
Figure 10. Distribution of risk categories.

According to the results of the current study as mentioned in Figure 11, Industry 4.0 had operational and implementation risks because it employed highly automated technology. With that in mind, Industry 5.0, which emphasizes a human-centric approach and uses advanced technologies like DT, cobots, 6G networks, etc., calls for people to develop competency skills. As they work with advanced robots, human workers must learn how to collaborate with smart machines. Learning technical and soft skills can be difficult for human workers, especially in emerging fields like overseeing translation and developing industrial robots [9]. Changes in organizational culture, business procedures, and job responsibilities are frequently necessary for the deployment of new technology. Important elements of operational and implementation risks include controlling change resistance and enabling smooth transitions.

Risks associated with the workforce and training are mostly related to the human resources side of integrating new technologies. These dangers are primarily focused on the individual and on how well the workforce can adopt and use the new technologies. People frequently struggle to adjust to new situations, and when forced to coexist alongside robots at work, they frequently struggle to do so. The adoption of cutting-edge technology necessitates greater time and effort from human workers. When procedures are often automated and advanced machines are utilized in Industry 4.0, there are workforce and training hazards. In Industry 5.0, it is also challenging to execute a human-centric strategy smoothly since humans find it difficult to work with robots. It is crucial to understand that there can still be obstacles in the way of this new paradigm's adoption. To guarantee a seamless and inclusive transformation, Industry 5.0 deployment demands a delicate balancing act between technology, employee development, and organizational culture.

Industry 4.0 also entails other dangers, such as those related to finances, society, system integration, and other factors. Investments in cutting-edge technology are essential since it is becoming more expensive for firms to train employees, which makes it difficult for them to upgrade their production lines for Industry 5.0 [9]. Industry 5.0 adoption is costly due to the need for smart machines and skilled staff to enhance production and efficiency.

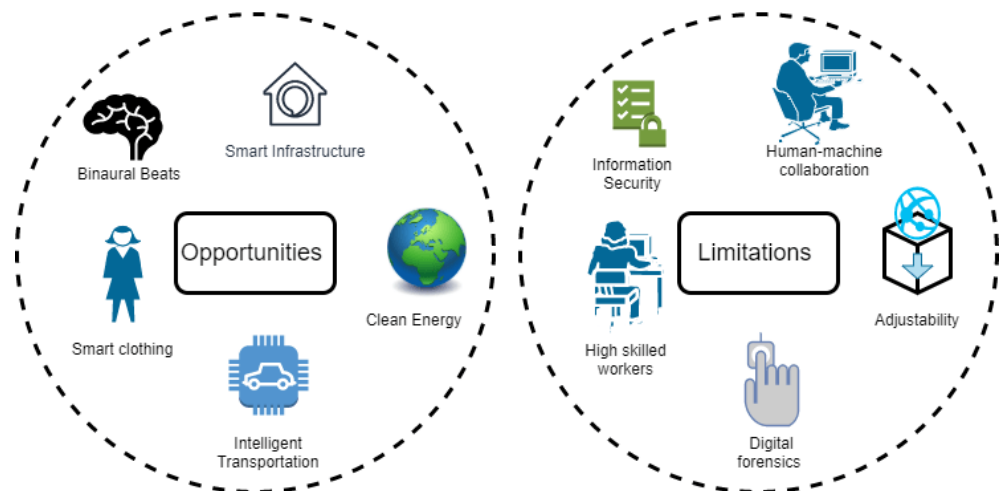
Other than these issues, one of the primary concerns in Industry 5.0 is the risk to human health. It has been shown from study papers that individuals are inclined to adapt to this because they feel uneasy using machines. The advent of new technology, such as collaborative robots and AI-driven systems, may leave the workforce unsure about the risks that could be involved. Because machines are playing a bigger role in the production process, workers may be concerned about mishaps or injuries. Industry standards and regulatory frameworks are crucial for ensuring safety and security in advanced industrial environments like Industry 5.0. These guidelines enforce safety measures for robotics, data privacy standards for AI-driven systems, and cybersecurity best practices for Internet of Things devices, ensuring a safe and uniform environment [61].



**Figure 11.** Highlights of the study.

## 6. Solution

As mentioned above, few pertinent studies, particularly high-quality journal papers, are accessible for reference because Industry 5.0 is a relatively new idea. Additionally, there are a variety of viewpoints on how Industry 5.0 will evolve, including the usage of various supporting technologies, worker training for the industrial transition, and the design of Industry 5.0 systems as shown in Figure 12. This has caused a lack of specific goals for the development of Industry 5.0 architecture and the application of associated enabling technologies.



**Figure 12.** Opportunities and Limitations in Industry 5.0 [9].

As a result of the numerous risks associated with Industry 4.0, Industry 5.0 is also conquering those risks. Some ways may mitigate these risks. Industry 4.0's IoT had numerous difficulties, but Industry 5.0 systems can be more autonomous and sustainable thanks to smart contracts implemented using blockchain technology, which also reduces the need for various types of documentation and third parties. Since the IIoT contains a lot of sensitive and important data that needs to be protected, resilient manufacturing techniques can help improve data security [34].

The necessity for technologies to adapt to the growing digitalization is one of the key problems of Industry 4.0. However, Industry 5.0 strives to be people-centric and blends human innovation with machine accuracy to boost performance and efficiency. It would be simple to adapt to Industry 5.0 provided workers received adequate training on the technologies [20].

The automation of current production technology is a result of Industry 4.0. Therefore, it is essential to give the employees proper training. Although Industry 5.0 emphasizes human centricity and is built on effective human-robot cooperation. Cobots have made a significant contribution in this regard. These robots cooperate with people to complete the assigned task. As a result, they assist in increasing the workers' productivity and efficiency. Without having to perform boring duties or risk their safety, the workforce can engage in more valuable activities. To guard against future failures, these devices must, however, undergo predictive maintenance [9].

Industry sectors, cybersecurity professionals, governmental organizations, and technology suppliers are working together to develop an Industry 5.0 environment that is resilient. Businesses are working with cybersecurity specialists to implement cutting-edge security measures and carry out in-depth risk assessments. This entails putting in place sophisticated intrusion detection systems, safe communication channels, and encryption techniques designed to safeguard assets in the rapidly changing Industry 5.0 environment [62]. Governmental organizations enforce cybersecurity standards, promote information exchange, and collaborate with technology providers to enhance Industry 5.0's

resilience. This collaboration strengthens defenses against cyberthreats and creates a safe, flexible industrial environment [63,64].

## 7. Applications

### 7.1. Manufacturing Industry

Industry 5.0 emphasizes maximizing collaboration between more accurate machinery and human creativity. To ensure sustainable production, it develops practices for resource recycling and reuse. It is also essential that production has less negative environmental effects [9]. Worldwide industrial processes are changing thanks to Industry 5.0, which frees human workers from boring tasks. In the past, robots have been used to complete dangerous, exhausting, or physically taxing jobs in production settings, such as welding, painting, and carrying big goods into warehouses. As office equipment becomes smarter and more networked, Industry 5.0 aims to combine cognitive computing capabilities with human intelligence and resourcefulness to facilitate collaborative tasks [20].

### 7.2. Education

The goal of Industry 4.0 education was to minimize human involvement and give emphasis to machines; however, the goal of Industry 5.0 education is to develop a synergy between autonomous machines and humans. Stronger equipment working in tandem with better-trained specialists will promote efficient, safe, and sustainable production [9].

### 7.3. Intelligent Healthcare

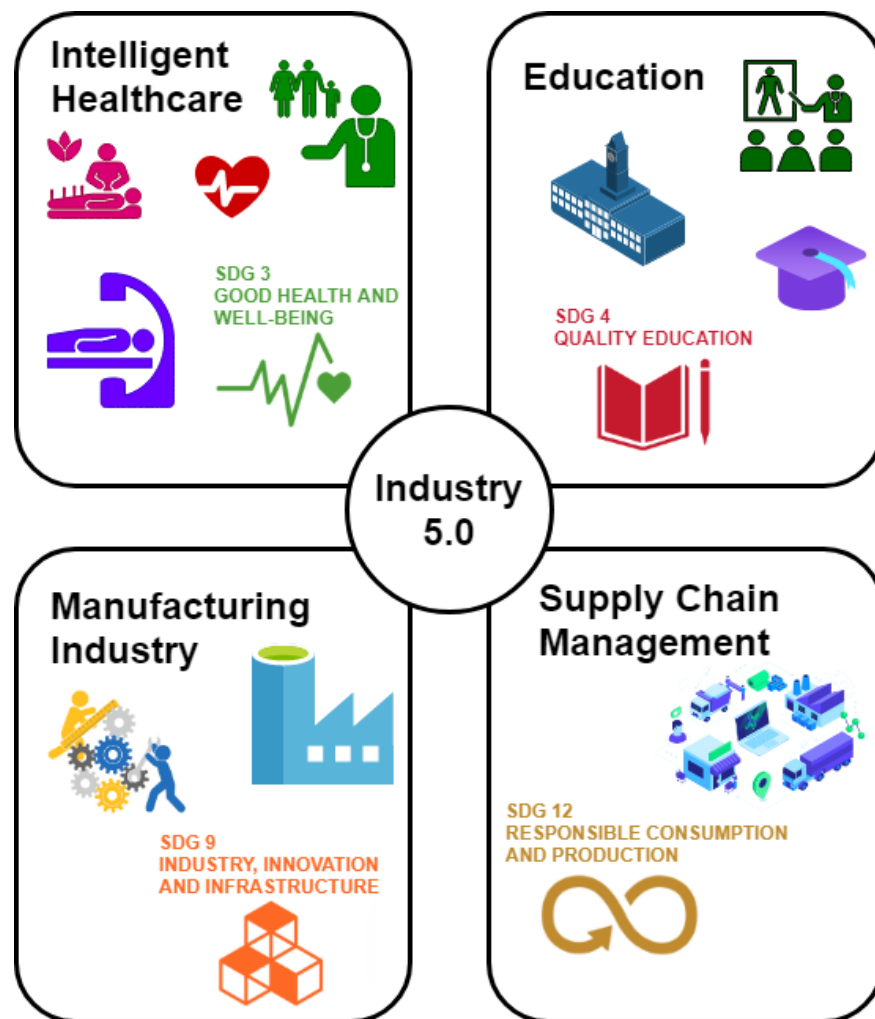
A real-time, intelligent hospital is what Industry 5.0 aims to build. Within the healthcare industry, technology can offer remote monitoring solutions. It is crucial to improving the doctors' quality of life. Doctors may concentrate on infected patients and give effective data for better treatment during the COVID-19 pandemic using this smart healthcare technology [9]. These days, doctors use ML models to aid in the diagnosis of patients' illnesses. Intelligent wearable, a patient's medical data can be continuously captured in real time by such smart watches and sensors and stored in the cloud [20].

### 7.4. Supply Chain Management

Industry 5.0-enabling disruptive technologies, such as DT, cobots, 5G and beyond, ML, and IoT, when combined with human ingenuity and smarts, can assist businesses in fulfilling demand for delivering personalized and customized goods more quickly. This assists supply chain management in integrating mass customization into their production processes since it is a fundamental tenant of Industry 5.0 [20]. Additionally, it guarantees that the supply chain's end-to-end operations are smooth, including the choice of raw materials based on an understanding of the demands of each customer in terms of customization and personalization. Industry 5.0 aims to integrate automated, intelligent digital ecosystems with human interaction, enhancing customer satisfaction and managing corporate productivity and profit margins through innovative supply chain solutions [9].

In Industry 5.0, there is a pronounced emphasis on achieving sustainable development goals (SDGs), specifically focusing on goals related to health and wellbeing (SDG 3), decent work and economic growth (SDG 8), industry, innovation, and infrastructure (SDG 9), and sustainable cities and communities (SDG 11), as depicted in Figure 13. These goals will be positively impacted by the development of Society 5.0 and the shift from Industry 4.0 to Industry 5.0. Novel business models, disaster management, and the digital transformation of healthcare are all aided by disruptive technology. Disruptive technologies also partially contribute to the achievement of other SDGs, including no poverty (SDG 1), zero hunger (SDG 2), high-quality education (SDG 4), clean water and sanitation (SDG 6), inexpensive and clean energy (SDG 7), and responsible consumption and production (SDG 12). Interactions among the SDGs have an indirect impact on the remaining objectives. Although Society 5.0 will firmly prioritize responsible consumption, Industry 5.0 will unavoidably lead to increased production, adaptability, and efficiency. Industry 5.0 and Society 5.0

are linked to smart city and village concepts, indicating their potential contributions to socio-economic sustainability as well as their influence on other SDGs [65].



**Figure 13.** Industry 5.0 Applications with Sustainable Development [9,20].

The research findings have significant theoretical and practical implications for organizations pursuing Industry 5.0 adoption. The study of three main risk categories—security, workforce and training, and operational and implementation—gives a strong theoretical basis for comprehending the risks inherent in the architecture of Industry 5.0. Drawing from previous research, the theoretical implications provide a thorough view of potential pitfalls beyond the synthesis of existing knowledge. This synthesis is a useful resource for academics and researchers examining the relationship between technology and industrial paradigms, and it also advances our theoretical knowledge of Industry 5.0 risks. From a practical standpoint, the identification of these risks provides practitioners with useful information to support their strategic planning and risk reduction initiatives. To protect sensitive data, practitioners can use the insights offered to strengthen their cybersecurity architecture, put strong encryption mechanisms in place, and set up proactive monitoring systems. A customized approach to breaking down the barrier between human–machine interaction is provided by identifying workforce and training concerns as organizations enter the Industry 5.0 scenario. The study emphasizes how important it is to fund training initiatives, close the knowledge gap, and develop a workforce capable of working in harmony with cutting-edge technologies. This reduces operational disturbances brought on by a shortage of human competence in addition to promoting an innovative culture. Moreover, the practical consequences are critical when it comes to operational and implementation

concerns. The lack of qualified employees to implement Industry 5.0 initiatives is a significant obstacle, and this study offers firms a road map to overcome it. This synthesis contributes to the academic discourse and provides industry professionals with practical counsel on navigating the challenges of Industry 5.0 adoption by balancing theoretical insights with practical considerations.

Production managers should prioritize an adequate cybersecurity architecture, fund ongoing training initiatives, and employ strategic ways to control operational risks, according to this study. These include adopting safe communication methods, putting strong encryption techniques into place, and incorporating real-time monitoring systems. Productivity and resilience can also be improved by creating a collaborative atmosphere that promotes human–machine synergy. Production managers can successfully incorporate Industry 5.0 into their operational frameworks by putting these recommendations into practice. This study sincerely attempted to discover and classify a wide range of potential obstacles with the goal of fully comprehending the risks landscape in Industry 5.0. It is recognized that the dynamic nature of Industry 5.0 may create new threats that are still unknown, even if every attempt was made to investigate and list the various concerns connected to the integration of modern technologies in industrial ecosystems. By carefully examining a broad range of risks in the context of Industry 5.0, the research aims to lay a solid foundation. Given the constant evolution of technology, it is critical to understand that new risks could emerge at any time. However, the risks that have been carefully detailed in this study provide insightful information that production managers need to know to make the transition to Industry 5.0. Production managers can use these insights to strengthen their preparation, effectively address obstacles, and make a substantial contribution to the overall success of Industry 5.0 integration in the manufacturing sector.

## 8. Limitations and Future Work

Technology's acceptance and technological trust are essential. People who use the new technologies are being trained at the same time as technology is being adapted to humans. Security, privacy, a lack of skilled staff, a drawn-out process, and a high price demand are the present problems. Industry 5.0 adoption is required to work with smart machines and cobots and adhere to industrial standards and laws. The three future directions for Industry 5.0 are quantum computing, cognitive computing, and human–machine interaction [9]. The installation phase of the technologies brought by Industry 5.0 is still ongoing. The literature research reveals their advantages over Industry 4.0; however, it does not mention any potential future difficulties. As a result, it is challenging to research the constraints and difficulties presented by Industry 5.0 technologies. Future research can be done to identify the difficulties Industry 5.0 technologies encounter and produce a workable solution [34].

Asset taxonomy and risk assessment methodologies must be modified as Industry 5.0 develops to account for future technological advances and scalability. Asset taxonomy, which groups and arranges different assets, must be adaptable enough to integrate new technology easily. To incorporate new categories like sophisticated robotics, AI-driven systems, and developing Industry 5.0-specific IoT devices, taxonomy frameworks must be continuously improved. As this report makes clear, there are still a lot of workforce and training risks, and people are still not prepared to adjust to Industry 5.0. Therefore, for people in this industry to be able to deal with machines with ease as time goes on, they must be adequately trained in accordance with technological changes.

## 9. Conclusions

This review-based work focuses on analyzing the difficulties that Industry 5.0 is facing. Industry 5.0 has implemented several new technical advances, including collaborative robotics, cyber-physical cognitive systems, hypercustomization in the industry, and predictive maintenance. This study paper examined Industry 5.0, its potential, and the difficulties it poses in the constantly changing context of the Industrial Revolution. Through automation, IoT, AI, and data-driven processes, Industry 4.0 paved the door for incredible



improvements, but it also exposed several hazards that required careful consideration. The study analyzed and highlighted hazards associated with Industry 4.0, including personnel and training risks, operational and implementation risks, and cybersecurity concerns. The panorama of industrial transformation has advanced further with the arrival of Industry 5.0, adopting a human-centric strategy that aims to balance humans and technology. It has been noted that the risks mentioned in Industry 4.0 have trickled down to Industry 5.0 despite this paradigm shift. Although Industry 5.0 offers hopeful glimpses of a new industrial age, it also encounters the same constraints, roadblocks, and difficulties as Industry 4.0. As networked systems and technology continue to be targets for malicious actors, the research demonstrated that cybersecurity dangers still exist in Industry 5.0. Operational and implementation risks continue to exist since the integration of sophisticated technology demands careful planning and adaptation to existing systems. In addition to presenting challenges for the workforce, Industry 5.0's seamless adoption of a human-centric strategy may make it difficult for people to interact with robots productively.

**Author Contributions:** Conceptualization, M.A.H. and S.Z.; methodology, M.A.H.; validation, S.Z., M.U.F., M.M.A. and S.A.N.; writing—original draft preparation, M.A.H.; writing—review and editing, M.A.H. and S.Z.; supervision, S.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Apriliyanti, M. Challenges of The Industrial Revolution Era 1.0 to 5.0: University Digital Library In Indoensia. *Libr. Philos. Pract.* **2022**, 1–17.
2. Yavari, F.; Pilevari, N. Industry revolutions development from Industry 1.0 to Industry 5.0 in manufacturing. *J. Ind. Strateg. Manag.* **2020**, 5, 44–63.
3. Castelo-Branco, I.; Oliveira, T.; Simões-Coelho, P.; Portugal, J.; Filipe, I. Measuring the fourth industrial revolution through the Industry 4.0 lens: The relevance of resources, capabilities and the value chain. *Comput. Ind.* **2022**, 138, 103639. [\[CrossRef\]](#)
4. Soori, M.; Arezoo, B.; Dastres, R. Internet of things for smart factories in industry 4.0, a review. *Internet Things Cyber-Phys. Syst.* **2023**, 3, 192–204. [\[CrossRef\]](#)
5. Akundi, A.; Euressti, D.; Luna, S.; Ankobiah, W.; Lopes, A.; Edinbarough, I. State of Industry 5.0—Analysis and identification of current research trends. *Appl. Syst. Innov.* **2022**, 5, 27. [\[CrossRef\]](#)
6. Zizic, M.C.; Mladineo, M.; Gjeldum, N.; Celent, L. From industry 4.0 towards industry 5.0: A review and analysis of paradigm shift for the people, organization and technology. *Energies* **2022**, 15, 5221. [\[CrossRef\]](#)
7. Golovianko, M.; Terziyan, V.; Branytskyi, V.; Malyk, D. Industry 4.0 vs. Industry 5.0: co-existence, Transition, or a Hybrid. *Procedia Comput. Sci.* **2023**, 217, 102–113. [\[CrossRef\]](#)
8. Gladysz, B.; Tran, T.a.; Romero, D.; van Erp, T.; Abonyi, J.; Ruppert, T. Current development on the Operator 4.0 and transition towards the Operator 5.0: A systematic literature review in light of Industry 5.0. *J. Manuf. Syst.* **2023**, 70, 160–185. [\[CrossRef\]](#)
9. Adel, A. Future of industry 5.0 in society: Human-centric solutions, challenges and prospective research areas. *J. Cloud Comput.* **2022**, 11, 40. [\[CrossRef\]](#) [\[PubMed\]](#)
10. Wang, B.; Zhou, H.; Li, X.; Yang, G.; Zheng, P.; Song, C.; Yuan, Y.; Wuest, T.; Yang, H.; Wang, L. Human Digital Twin in the context of Industry 5.0. *Robot. Comput.-Integr. Manuf.* **2024**, 85, 102626. [\[CrossRef\]](#)
11. Paschek, D.; Mocan, A.; Draghici, A.; et al. Industry 5.0—The expected impact of next industrial revolution. In Proceedings of the Thriving on Future Education, Industry, Business, and Society, Piran, Slovenia, 15–17 May 2019; MakeLearn and TIIM International Conference; pp. 15–17.
12. Longo, F.; Padovano, A.; Umbrello, S. Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future. *Appl. Sci.* **2020**, 10, 4182. [\[CrossRef\]](#)
13. Ghobakhloo, M.; Iranmanesh, M.; Mubarak, M.F.; Mubarik, M.; Rejeb, A.; Nilashi, M. Identifying industry 5.0 contributions to sustainable development: A strategy roadmap for delivering sustainability values. *Sustain. Prod. Consum.* **2022**, 33, 716–737. [\[CrossRef\]](#)

14. Grabowska, S.; Saniuk, S.; Gajdzik, B. Industry 5.0: improving humanization and sustainability of Industry 4.0. *Scientometrics* **2022**, *127*, 3117–3144. [\[CrossRef\]](#) [\[PubMed\]](#)
15. Moroa, S.; Cauchick-Miguel, P.; de Sousa-Zomerb, T.; de Sousa Mendesc, G. Design of a sustainable electric vehicle sharing business model in the Brazilian context. *Int. J. Ind. Eng. Manag. (IJIEEM)* **2023**, *14*, 147–161. [\[CrossRef\]](#)
16. Jankovic-Zugic, A.; Medic, N.; Pavlovic, M.; Todorovic, T.; Rakic, S. Servitization 4.0 as a Trigger for Sustainable Business: Evidence from Automotive Digital Supply Chain. *Sustainability* **2023**, *15*, 2217. [\[CrossRef\]](#)
17. Sofic, A.; Rakic, S.; Pezzotta, G.; Markoski, B.; Arioli, V.; Marjanovic, U. Smart and Resilient Transformation of Manufacturing Firms. *Processes* **2022**, *10*, 2674. [\[CrossRef\]](#)
18. Dave, D.M. Advancing Resilience and Agility in Manufacturing through Industry 5.0: A Review of Digitization, Automation, and Advanced Analytics. *Int. J. New Technol. Res. (IJNTR)* **2023**, *9*, 5–12.
19. Alves, J.; Lima, T.M.; Gaspar, P.D. Is Industry 5.0 a Human-Centred Approach? A Systematic Review. *Processes* **2023**, *11*, 193. [\[CrossRef\]](#)
20. Maddikunta, P.K.R.; Pham, Q.V.; Prabadevi, B.; Deepa, N.; Dev, K.; Gadekallu, T.R.; Ruby, R.; Liyanage, M. Industry 5.0: A survey on enabling technologies and potential applications. *J. Ind. Inf. Integr.* **2022**, *26*, 100257. [\[CrossRef\]](#)
21. Turner, C.J.; Garn, W. Next generation DES simulation: A research agenda for human centric manufacturing systems. *J. Ind. Inf. Integr.* **2022**, *28*, 100354. [\[CrossRef\]](#)
22. Eriksson, K.; Alsaleh, A.; Behzad Far, S.; Stjern, D. Applying Digital Twin Technology in Higher Education: An Automation Line Case Study. *Adv. Transdiscipl. Eng* **2022**, *21*, 461–472.
23. Pozo, E.; Patel, N.; Schrödel, F. Collaborative Robotic Environment for Educational Training in Industry 5.0 Using an Open Lab Approach. *IFAC-PapersOnLine* **2022**, *55*, 314–319. [\[CrossRef\]](#)
24. Fatima, Z.; Tanveer, M.H.; Waseemullah.; Zardari, S.; Naz, L.F.; Khadim, H.; Ahmed, N.; Tahir, M. Production plant and warehouse automation with IoT and industry 5.0. *Appl. Sci.* **2022**, *12*, 2053. [\[CrossRef\]](#)
25. Clim, A. Cyber security beyond the Industry 4.0 era. A short review on a few technological promises. *Inform. Econ.* **2019**, *23*, 34–44. [\[CrossRef\]](#)
26. Toma, A.; Constantinescu, R.; Zota, R. Enhancing administrative services through document models. In Proceedings of the 5th International Conference Knowledge Management: Projects, Systems and Technologies, Bucuresti, Romania, 12–13 November 2010 ; pp. 94–102.
27. Tinica, G.; Bostan, I.; Grosu, V. The dynamics of public expenses in healthcare and demographic evolution in Italy and Romania. *Rev. Romana Bioet.* **2008**, *6*, 48–63.
28. Kamel, S.O.M.; Hegazi, N.H. A proposed model of IoT security management system based on a study of internet of things (IoT) security. *Int. J. Sci. Eng. Res.* **2018**, *9*, 1227–1244.
29. Sanmartin, P.; Rojas, A.; Fernandez, L.; Avila, K.; Jabba, D.; Valle, S. Sigma routing metric for RPL protocol. *Sensors* **2018**, *18*, 1277. [\[CrossRef\]](#) [\[PubMed\]](#)
30. Waslo, R.; Lewis, T.; Hajj, R.; Carton, R. Industry 4.0 and cybersecurity: Managing risk in an age of connected production. *Erişim tarihi* **2017**, *15*.
31. Pedreira, V.; Barros, D.; Pinto, P. A review of attacks, vulnerabilities, and defenses in industry 4.0 with new challenges on data sovereignty ahead. *Sensors* **2021**, *21*, 5189. [\[CrossRef\]](#) [\[PubMed\]](#)
32. Huang, S.; Wang, B.; Li, X.; Zheng, P.; Mourtzis, D.; Wang, L. Industry 5.0 and Society 5.0—Comparison, complementation and co-evolution. *J. Manuf. Syst.* **2022**, *64*, 424–428. [\[CrossRef\]](#)
33. Leng, J.; Zhong, Y.; Lin, Z.; Xu, K.; Mourtzis, D.; Zhou, X.; Zheng, P.; Liu, Q.; Zhao, J.L.; Shen, W. Towards resilience in Industry 5.0: A decentralized autonomous manufacturing paradigm. *J. Manuf. Syst.* **2023**, *71*, 95–114. [\[CrossRef\]](#)
34. Khan, M.; Haleem, A.; Javaid, M. Changes and improvements in Industry 5.0: A strategic approach to overcome the challenges of Industry 4.0. *Green Technol. Sustain.* **2023**, *1*, 100020. [\[CrossRef\]](#)
35. Sklyar, V.; Kharchenko, V. ENISA documents in cybersecurity assurance for industry 4.0: IIoT threats and attacks scenarios. In Proceedings of the 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 8–21 September 2019; Volume 2, pp. 1046–1049.
36. Sanchez, D.O.M. Sustainable development challenges and risks of Industry 4.0: A literature review. In Proceedings of the Global IoT Summit (GloTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6.
37. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artif. Intell. Rev.* **2021**, *54*, 3849–3886. [\[CrossRef\]](#)
38. Rubio, J.E.; Roman, R.; Lopez, J. Analysis of cybersecurity threats in industry 4.0: the case of intrusion detection. In Proceedings of the Critical Information Infrastructures Security: 12th International Conference—CRITIS 2017, Lucca, Italy, 8–13 October 2017; Revised Selected Papers 12; pp. 119–130.
39. Prinsloo, J.; Sinha, S.; von Solms, B. A review of industry 4.0 manufacturing process security risks. *Appl. Sci.* **2019**, *9*, 5105. [\[CrossRef\]](#)
40. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [\[CrossRef\]](#)
41. Mullet, V.; Sondi, P.; Ramat, E. A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [\[CrossRef\]](#)

42. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
43. Radanliev, P.; De Roure, D.; Page, K.; Nurse, J.R.; Mantilla Montalvo, R.; Santos, O.; Maddox, L.; Burnap, P. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity* **2020**, *3*, 2020. [CrossRef]
44. Rudenko, R.; Pires, I.M.; Oliveira, P.; Barroso, J.; Reis, A. A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity. *Electronics* **2022**, *11*, 1742. [CrossRef]
45. Tamvada, J.P.; Narula, S.; Audretsch, D.; Puppala, H.; Kumar, A. Adopting new technology is a distant dream? The risks of implementing Industry 4.0 in emerging economy SMEs. *Technol. Forecast. Soc. Chang.* **2022**, *185*, 122088. [CrossRef]
46. Sweeney, D.; Nair, S.; Cormican, K. Scaling AI-based industry 4.0 projects in the medical device industry: An exploratory analysis. *Procedia Comput. Sci.* **2023**, *219*, 759–766. [CrossRef]
47. Capodiec, A.; Mainetti, L.; Dipietrangelo, F. Model-Driven approach to Cyber Risk Analysis in Industry 4.0. In Proceedings of the 10th International Conference on Information Systems and Technologies, Lecce, Italy, 4–5 June 2020; pp. 1–7.
48. Rezqianita, B.L.; Ardi, R. Drivers and barriers of industry 4.0 adoption in Indonesian manufacturing industry. In Proceedings of the 3rd Asia Pacific Conference on Research in Industrial and Systems Engineering, Depok, Indonesia, 16–17 June 2020; pp. 123–128.
49. Digmayer, C.; Jakobs, E.M. Employee Empowerment in the Context of domain-specific Risks in Industry 4.0. In Proceedings of the IEEE International Professional Communication Conference (ProComm), Toronto, ON, Canada, 22–25 July 2018; pp. 125–133.
50. Kurt, R. Industry 4.0 in terms of industrial relations and its impacts on labour life. *Procedia Comput. Sci.* **2019**, *158*, 590–601. [CrossRef]
51. Zimmermann, M.; Rosca, E.; Antons, O.; Bendul, J.C. Supply chain risks in times of Industry 4.0: Insights from German cases. *IFAC-PapersOnLine* **2019**, *52*, 1755–1760. [CrossRef]
52. Leng, J.; Sha, W.; Wang, B.; Zheng, P.; Zhuang, C.; Liu, Q.; Wuest, T.; Mourtzis, D.; Wang, L. Industry 5.0: Prospect and retrospect. *J. Manuf. Syst.* **2022**, *65*, 279–295. [CrossRef]
53. Polak-Sopinska, A.; Wisniewski, Z.; Walaszczyk, A.; Maczewska, A.; Sopinski, P. Impact of industry 4.0 on occupational health and safety. In *Advances in Manufacturing, Production Management and Process Control, Proceedings of the AHFE 2019 International Conference on Human Aspects of Advanced Manufacturing, and the AHFE International Conference on Advanced Production Management and Process Control, Washington DC, USA 24–28 July 2019*; Springer: Cham, Switzerland, 2020; pp. 40–52.
54. Barraza de la Paz, J.V.; Rodríguez-Picón, L.A.; Morales-Rocha, V.; Torres-Argüelles, S.V. A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems* **2023**, *11*, 218. [CrossRef]
55. Raj, A.; Dwivedi, G.; Sharma, A.; de Sousa Jabbour, A.B.L.; Rajak, S. Barriers to the adoption of industry 4.0 technologies in the manufacturing sector: An inter-country comparative perspective. *Int. J. Prod. Econ.* **2020**, *224*, 107546. [CrossRef]
56. Pacaux-Lemoine, M.P.; Trentesaux, D. Ethical risks of human-machine symbiosis in industry 4.0: Insights from the human-machine cooperation approach. *IFAC-PapersOnLine* **2019**, *52*, 19–24. [CrossRef]
57. Bragança, S.; Costa, E.; Castellucci, I.; Arezes, P.M. A brief overview of the use of collaborative robots in industry 4.0: Human role and safety. In *Occupational and Environmental Safety and Health*; Springer: Cham, Switzerland, 2019; pp. 641–650.
58. Rea-Guaman, A.; San Feliu, T.; Calvo-Manzano, J.; Sánchez-García, I.D. Systematic review: Cybersecurity risk taxonomy. In *Trends and Applications in Software Engineering, Proceedings of the 6th International Conference on Software Process Improvement (CIMPS 2017), Zacatecas, Mexico, 18–20 October 2017*; Springer: Cham, Switzerland, 2018; pp. 137–146.
59. Jarrow, R.A. Operational risk. *J. Bank. Financ.* **2008**, *32*, 870–879. [CrossRef]
60. Lee, J.; Bagheri, B.; Kao, H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
61. Nah, E.H.; Cho, S.; Kim, S.; Cho, H.I.; Stingu, C.S.; Eschrich, K.; Thiel, J.; Borgmann, T.; Schaumann, R.; Rodloff, A.C.; et al. International organization for standardization (ISO) 15189. *Ann. Lab. Med.* **2017**, *37*, 365–370.
62. Kalloniatis, C.; Kavakli, E.; Gritzalis, S. Addressing Privacy in Traditional and Cloud-Based Systems. *Int. J. Appl. Ind. Eng. (IJAIE)* **2014**, *2*, 14–40. [CrossRef]
63. Ateş, A.; Açıkbay, S.; Söylemez, M.T. Comparison of Disturbance Resolution between Timetable and Headway Based Regulations in CBTC: A Case Study of Marmaray. In Proceedings of the 11th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 28–30 November 2019; pp. 1060–1065.
64. Cybersecurity, C.I. Framework for Improving Critical Infrastructure Cybersecurity. 2018. Available online: <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf> (accessed on 18 December 2023).
65. Kasinathan, P.; Pugazhendhi, R.; Elavarasan, R.M.; Ramachandaramurthy, V.K.; Ramanathan, V.; Subramanian, S.; Kumar, S.; Nandhagopal, K.; Raghavan, R.R.V.; Rangasamy, S.; et al. Realization of Sustainable Development Goals with Disruptive Technologies by Integrating Industry 5.0, Society 5.0, Smart Cities and Villages. *Sustainability* **2022**, *14*, 15258. [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.