Discover Applied Sciences

Review

Navigating contemporary challenges and future prospects in digital industry evolution

Maryam Gallab[1] · Mario Di Nardo[2] · Lina Naciri[1]

Received: 8 January 2024 / Accepted: 24 April 2024

Abstract

The advent of the digital industry, also known as Industry 4.0 is a transformation period in manufacturing, where the integration of digital technologies with physical systems is underlined. This transformation is crucial for the pillars of cyber-physical systems (CPS), cyber resilience protection, and workers' safety, which collectively from the cornerstone of Industry 4.0. Ensuring the secure exploitation of Industry 4.0's advantages necessitates a dedicated focus on workers' safety, cyber resilience protection, and the security and privacy of human-centric CPS systems. However, the full realization of Industry 4.0's potential hinges upon effectively addressing these challenges and aligning the benefits of digitalization with the exigencies of worker well-being and safeguarding critical infrastructure. This study is a comprehensive literature review on this digital era, focusing on CPS, resilience, and workers' safety. The review aims to summarise current research and advancements, offering insights for researchers, practitioners, and decision-makers. By identifying gaps in knowledge, the study lays the foundations for additional research and supports ongoing progress in the digital industry. Industry 4.0 embodies a new era of manufacturing integrating digital technologies with a focus on sustainability and human-centric design, supported by CPS, resilience, and worker's safety. This necessitate addressing challenges to ensure benefits align with worker needs and infrastructure protection.

Article Highlights

- Systematic literature review to identify relevant keywords in the digital era such as Cyber-physical systems, resilience, and workers' safety.
- Role of resilience in the smart industry, cyber systems' responsibilities, safety in the human–robot interface, and the foundational elements of the digital industry.
- Need for comprehensive solutions that address not only technical aspects but also the psychological dimensions of safety in industrial systems.

Keywords Digital industry · Industry 4.0 · Safety · Smart factory · Resilience · Literature review · Cyber-physical systems (CPS) · Workers' safety

---

✉ Maryam Gallab, gallab@enim.ac.ma; Mario Di Nardo, mario.dinardo@unina.it; Lina Naciri, lina.naciry@gmail.com | [1]MIS-LISTD Laboratory, Computer Science Department, Mines-Rabat School (ENSMR), 10000 Rabat, Morocco. [2]Department of Chemical, Materials and Production Engineering, University of Naples Federico II, 80125 Naples, Italy.

Discover

1 Introduction

Recently, the principle of manufacturing is changing so deeply that is nowadays called "the fourth industrial revolution". The twenty-first century saw the start of this revolution in Hannover, Germany, which continues to outpace the digital revolution. However, let's consider that every machine and system in the Fourth Industrial Revolution uses digital objects and comprises numbers (0 and 1). We can refer to this time period as "The Age of Digital Objects". Implementing novel manufacturing techniques and the mechanisation of the sector by steam-powered equipment during the eighteenth and nineteenth centuries helped promote capital accumulation. Periodic changes from that era are known as an industry revolution. The first Industrial Revolution (which has seen the light in the United Kingdom) represents a fundamental shift from the agricultural economy to manufacturing. The establishment of factories using electrical energy and carrying out mass production signalled the beginning of the second phase of this fundamental revolution. Information and communication technology (ICT) systems were adapted for industrial operations in the late 1960s, which aided in the automation of production [1, 2].

We are currently in the fourth stage of this revolution. This revolution saw the acceleration of mechanical processes through the use of software and revolutionary technologies like artificial intelligence (AI), Internet of Things (IoT), and full-scale robotics of self-driving and unmanned vehicles; so, it brought a dramatic decrease in the human element's contribution while increasing the speed with which production was made by making very large calculations. The development of the internet, software, and hardware technologies paved the path for the creation of interoperable, communicable, and responsive objects. In this context, this revolution has seen a number of appointments: 4th revolution, Industry 4.0, Smart Manufacturing, Digital Industry, Intelligent Factory or Advanced Manufacturing [2].

Indeed, Industry 4.0 led manufacturing environments to digitalisation and automation. Same is applied to the supply chain supporting products, their business context, order prediction, delivery, retail, and potential customers [3] so, the notion "Industry 4.0" is proper to the fourth industrial revolution, a technology-driven industrial production wave that promises to revolutionise the way manufacturing is done.

It is based on a new generation of mobile internet technologies, faster and more adaptable characteristics of the Internet, and the creation of intelligent industrial robots by developing equipment connected to this global network. Robots, smart readers (sensors), unmanned vehicles, and other devices that we can categorise as components of each component and interact with online [4].

The advantages of Industry 4.0 include demand-driven manufacturing, efficient resource management, fault tolerance, autonomous operations reducing human errors, and the development of intelligent, customizable products. This fosters workplace satisfaction, dynamic decision-making, and customer-centric production. However, challenges involve the need for intelligent decision-making machinery, continuous connectivity, big data handling, control methods, security measures, and managerial challenges such as initial investment and more skilled workers. Despite these drawbacks, Industry 4.0 offers resilient and sustainable manufacturing with enhanced product quality and customer satisfaction [5, 6].

In conclusion, Industry 4.0, or the Digital industry, is set to revolutionise manufacturing. Using advanced technologies will help manufacturers improve efficiency, reduce costs, and improve the environment. With the help of Industry 4.0, manufacturers can stay competitive in an ever-changing world.

However, Industry 4.0 is only the beginning. Industry 5.0 is expected to be the next revolution, bringing even more advanced technologies and automation to the factory floor. Industry 5.0, on the other hand, relies on advances of Industry 4.0 and targets the development of advanced artificial intelligence and machine learning technologies [7]. This will enable manufacturers to automate more complex processes, further reducing costs and improving efficiency in appliances with resilience.

Therefore, this research interest is to serve as a referential to develop adaptive skills and overcome adverse situations, as, with "The Age of Digital Objects" comes the necessity to expand the limits and be able to react effectively, all while maintaining a strong level of stability.

To commence our research, we initiated a comprehensive bibliographic study involving the analysis of several pertinent articles. This initial phase aimed to acquire a deep understanding of the existing literature on Industry 4.0, digitalization, and related technologies. Subsequently, we meticulously selected and merged relevant articles, integrating them with strategically chosen keywords. This process was the foundation for formulating specific research questions (RQs) to guide our subsequent literature review.

The formulated research questions are as follows:

RQ1: How does resilience contribute to enhancing adaptability, robustness, and recovery mechanisms within the smart industry?

RQ2: In the digital industry, where specifically does the responsibility of cyber systems lie, and how does this impact the overall functioning and security of the digital ecosystem?

RQ3: What specific functions does safety serve in the human–robot interface within the Digital Industry, and how does it contribute to ensuring secure and efficient interactions between humans and robots?

RQ4: What specific components constitute the foundational elements of the digital industry, and how do these elements anticipate evolution in the future landscape of digitalization and industrial advancements as of Industry 5.0?

Following the establishment of these research questions, our team embarked on a systematic literature review. This methodical process involved not only scrutinizing published articles but also reviewing existing reviews on the subject matter. By delving into a diverse array of sources, we aimed to compile a comprehensive overview of the current state of knowledge regarding the intersection of Industry 4.0, digitalization, and associated themes.

This literature review, focusing on the selected keywords relevant to the digital age, is designed to serve multiple purposes. Firstly, it seeks to synthesize existing knowledge, combining insights from various scholarly perspectives. Secondly, the review aims to identify gaps in the current literature, pinpointing areas for further research. Finally, by distilling valuable information from the literature, we endeavour to provide a resource that proves beneficial not only to researchers but also to practitioners and policy-makers navigating the dynamic landscape of the digital era. Through this multifaceted approach, we aspire to contribute substantively to the ongoing discourse surrounding Industry 4.0 and its implications for resilience, cyber systems, safety in human–robot interfaces, and the foundational elements shaping the digital industry's future trajectory.

2 Methodology

The Scopus database searched for and selected relevant articles, excluding conference papers.

We carried out a systematic review, the framework adopted is shown in Fig. 1, which indicates that the study began with the research of the Industry 4.0 technologies. Further, some topics have been addressed, like resilience in the digital industry, advantages and disadvantages of Industry 4.0, cyber-physical systems, human–robot relationship, cyber resilience protection, workers' safety, and industry 5.0 techniques.

The central part of the survey presents the answers to the research question proposed.

Finally, conclusions, implications, and perspectives of the study were derived.

3 Review protocol

Accurate drafting of literature analysis is based on compliance with a rigorous standardised work protocol developed by a group of experts in 2005 and known by the acronym of PRISMA (Preferred Reporting Items for Systematic reviews and Me-ta-Analyses) Statement described by [8, 73]. Since then, and decades after launching its last version, PRISMA was majorly updated (Fig. 1).

4 Databases, keywords, inclusion criteria

Information collection developed in this paper was carried out through a systematic review of the literature, allowing an exhaustive knowledge of the state of the art relating to the subject matter. The first step was to identify a clear and effective studies localisation, selection, and inclusion strategy. Next, studies research relevant to the railway safety topic was carried out by placing specific queries on the Scopus database (http://www.scopus.com). Queries consist of entering specific keywords in the search engine: "Resilience", "Industry 4.0", "Safety", "Smart factory", "Industry 5.0". Scopus was chosen for this study for its popularity and because of its coverage of a wide range of articles in various disciplines, including literature review works. To avoid confusion, the study will focus only on the terms "Industry 4.0" and "Industry 5.0" to designate the digital industry.

Queries chosen for the acquisition of the working database are listed below in chronological order and illustrated in Fig. 2:

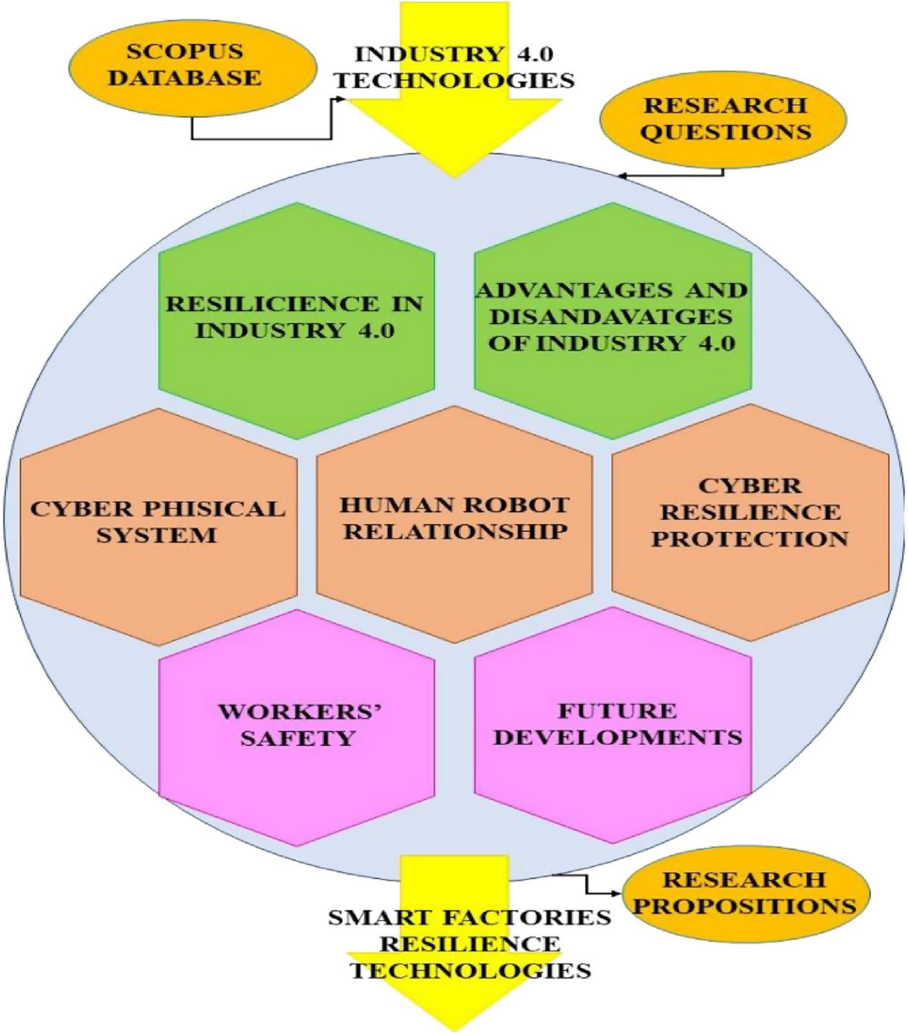
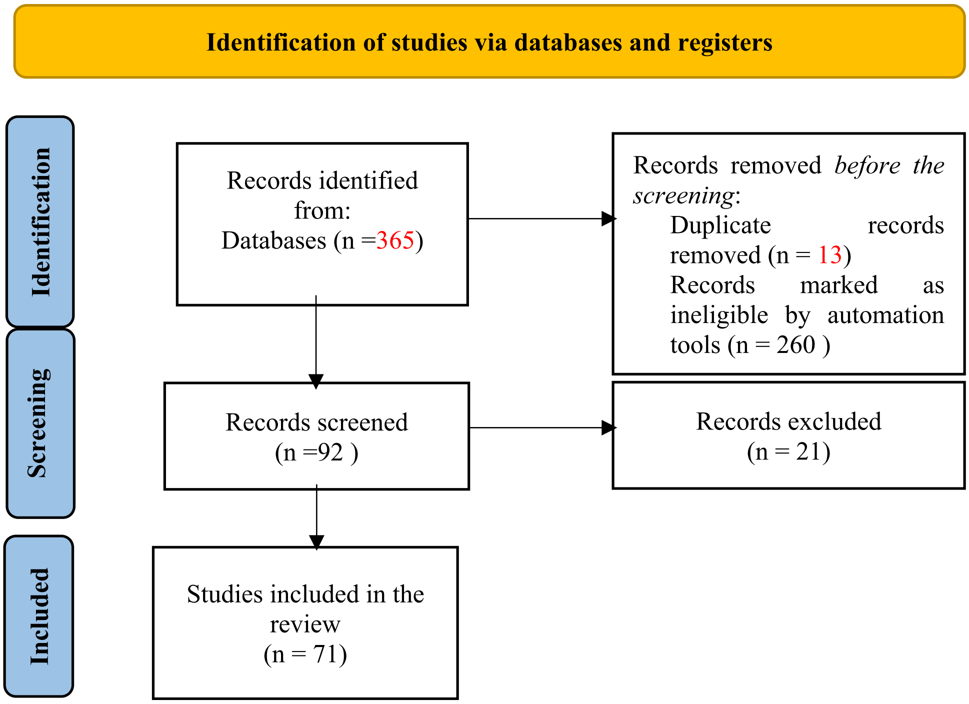


Fig.1 Framework used for the study of Digital Industry (Industry 4.0 / 5.0)

- Query 1: "Resilience", "Industry 4.0", "Safety" in tiles-abstracts-keywords. This search returns 44 documents. The publication window was restricted to the years 2019 through 2023. Additionally, only the English language was used in the studies. Only scientific reviews and articles are considered (f.e. conference papers were excluded). The result is 21 documents as a result of these restrictions.
- Query 2: "Industry 4.0", "Safety", "Smart factory" in tiles-abstracts-keywords. This search returns 84 documents. The publication window was restricted to the years 2019 through 2023. Additionally, only the English language was used in the studies. Only scientific reviews and articles are considered (f.e. conference papers were excluded). The result is 19 documents as a result of these restrictions.
- Query 3: "Industry 5.0", "Safety", "Resilience" in tiles-abstracts-keywords. This search returns 4 documents. The publication window was restricted to the years 2019 through 2023. Additionally, only the English language was used in the studies. Only scientific reviews and articles are taken into consideration (f.e. conference papers were excluded). The result is 4 documents as a result of these restrictions.
- Query 4: "Industry 4.0", "Safety", "Worker's safety" in tiles-abstracts-keywords. This search returns 44 documents. The publication window was restricted to the years 2019 through 2023. Additionally, only the English language was used in the studies. Only scientific reviews and articles are considered (f.e. conference papers were excluded). The result is 9 documents as a result of these restrictions.
- Query 5: "Industry 4.0", "Safety", "Cyber physical systems" in tiles-abstracts-keywords. This search returns 189 documents. The publication window was restricted to the years 2019 through 2023. Additionally, only the English language was used in the studies. Only scientific reviews and articles are taken into consideration (f.e. conference papers were excluded). The result is 39 documents as a result of these restrictions.

Fig. 2 PRISMA 2020 flow diagram for new systematic reviews, which included searches of databases and registers only



4.1 Classification

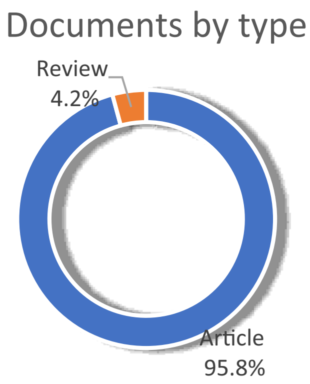
All 71 papers of the database obtained previously have been classified into two types (Fig. 3):

1. Article papers (68), i.e., original research is reported in articles referred to as empirical or primary sources. An introduction, sections describing the procedures, and sections summarising the findings will normally be present.
2. Review papers (3): i.e., papers synthesise or analyse research that has already been undertaken in primary sources and are sometimes referred to as literature reviews or secondary sources. They often provide an overview of the state of the research on a certain subject.

4.2 Keywords analysis

This paragraph analyses all the various keywords obtained from the database creation. The results obtained correspond to those expected; the keywords most present, "Industry 4.0"," Safety", "Cyber physical systems" and "Internet of things", are those used to research various queries. A possible observation is that keywords such as "Smart factory" and "Accident prevention" are also very frequent. Looking at the pictures (Fig. 4; Fig. 5) obtained respectively thanks to an R library, VOSviewer and

Fig.3 Type of paper



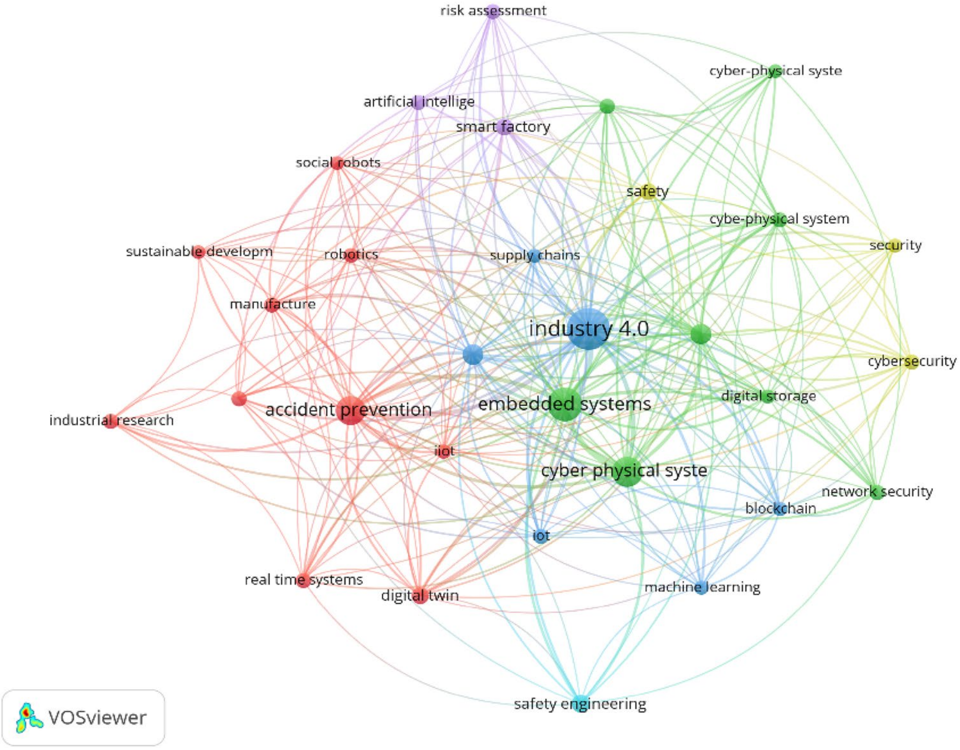


Fig. 4 Overlay Visualisation of top keywords used in the articles

Fig.5 The world cloud of the top keywords used in the selected articles

Bibliometrix, it is possible to note the relevance of keywords and the link between them: the thicker the arrow, the greater link between keywords.

4.3 Authorship and collaboration

The total number of authors who worked on publishing the papers collected in the database is 292.

In Fig. 6, thanks to R software, there is the link to co-authorship.

In Fig. 7 are reported the count of papers by state and their geographic distribution.

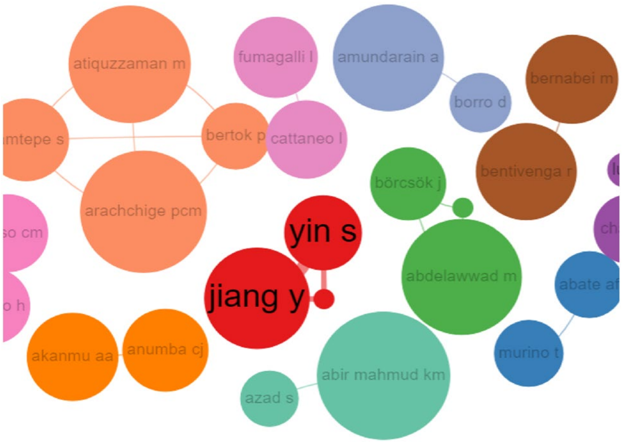


Fig. 6 Overlay visualisation of author collaboration in the articles

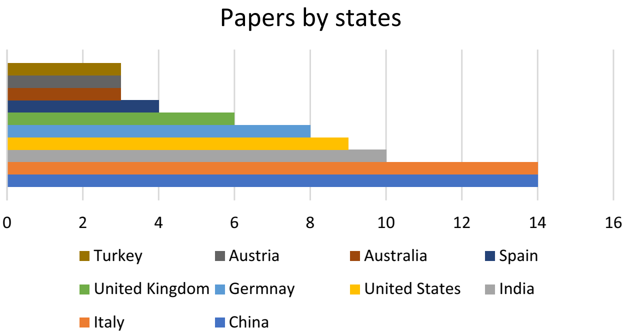


Fig.7 Papers by States

5 Thematic analysis

5.1 Resilience in industry 4.0

Entrepreneurial resilience is a critical facet of a business's ability to weather external shocks or disturbances within the socio-economic and political landscape. It encapsulates the capacity to adapt to new circumstances, remain stable in the face of external forces, and either revert to the initial condition or adopt a new equilibrium. This resilience is essential for tolerating outside pressures and ensuring long-term survival within dynamic markets.

Resilience, in its essence, is the ability to adapt swiftly while retaining the capacity to act. It involves a readiness to fundamentally rethink structures and processes when required. Conversely, robustness expresses a company's ability to face change without altering its fundamental structure. It is crucial to recognize that those who view a return to the pre-crisis system as necessary and believe that current difficulties have mostly been resolved may hold a fundamental misconception. Resilience is an ongoing strategic effort by company management to maintain long-term sustainability. It is not a one-time solution but a continuous commitment. Only resilient businesses, understanding the need for perpetual adaptation, are adequately prepared for the impending challenges that may arise [9].

As we delve into the dynamics of the Fourth Industrial Revolution, we see that it is propelled by many factors that will inevitably shape its trajectory. One of these factors is the ubiquitous use of mobile devices, particularly smartphones and tablets, in daily life. Emerging applications are envisioned to allow users to remotely control various devices and systems from their mobile devices, thereby further simplifying and integrating technology into our daily lives [10].

Networking and Internet Technologies are evolving rapidly, with IPv6 facilitating faster and more extensive data transfer across computer networks. This advancement anticipates a future where the swift and easy transfer of large amounts of data, video, and music across networks becomes a norm in day-to-day life. The connectivity of nearly every technological device to the internet foresees the emergence of a network society [10].

Cloud computing systems address the challenges associated with the increasing number of computing systems and devices used daily. These systems grapple with the need to store the vast amount of data these devices generate.

The resolution of this challenge involves leveraging cloud computing technologies for comprehensive, resilient, complete, and dependable data storage. The data stored in the cloud holds immense value due to its perpetual accessibility and immunity to loss or corruption [10].

The advent of big data is a direct outcome of automated processes that accumulate vast datasets beyond the capacity of manual management. Collecting, processing, and presenting data in extensive systems, such as e-government, necessitate in-depth work. This involves the identification and analysis of data with the necessary attributes. The introduction of a particular type of system called the System of Systems (SOS) represents a paradigm shift. SOS refers to associations of operational and managerial independent software-intensive systems distributed across various contexts. These systems, characterized as software-intensive, information-intensive, embedded, and ultra-large, collaborate to achieve high-level missions that cannot be accomplished by any single system alone. The need for collaboration emphasizes the development of architectures like Media Arch within the SOS framework [11].

The integration of Artificial Intelligence (AI) and Industrial Robots into various industries is witnessing exponential growth. Robots equipped with AI can communicate with one another and actively contribute to the production process. The future envisions robots dominating every production sector due to diverse applications of advanced decision-making algorithms [10].

Three-dimensional (3D) Printers mark a departure from traditional printers, enabling the rapid production of any industrial product. The versatility of these printers allows for the construction of spare parts and necessary modifications using three-dimensional drawings. This innovation has significant implications for the manufacturing industry. For instance, Ford utilized 3D printers during the development of the 2017 Mustang in the United States, underscoring the cost-effectiveness of this production method [10].

In the realm of Industry 4.0, the goal is to realize "smart factories" that incorporate advanced automation, robotics, big data analytics, and the Internet of Things (IoT). This paradigm shift is anticipated to revolutionize manufacturing processes, from design and production to the management and operation of factories [12]. The connectivity of machines, production lines, warehouses, and other elements of the factory environment to the Internet enables real-time insights into production processes. This connectivity facilitates the identification of areas where efficiency can be improved. By embracing Industry 4.0, manufacturers can streamline processes, reduce costs, and enhance productivity.

Beyond the operational improvements, Industry 4.0 offers several additional benefits. Using data and analytics allows for more accurate forecasting of demand and production. This, in turn, enables manufacturers to better meet customer needs while simultaneously reducing inventory costs. The integration of the latest advances in robotics and automation has the potential to minimize the need for manual labour, creating safer and more efficient working environments. Importantly, Industry 4.0 is expected to have positive environmental impacts by reducing production's energy and resource requirements. Additionally, manufacturers can reduce their reliance on harmful chemicals and pollutants through the use of cutting-edge technologies [13].

In conclusion, entrepreneurial resilience is fundamental for businesses navigating the ever-evolving external landscape. The Fourth Industrial Revolution, propelled by technological advancements, is reshaping industries and manufacturing processes. Each component plays a crucial role in this transformative journey, from the ubiquity of mobile devices to the integration of AI and robotics. Industry 4.0 represents a shift towards smarter factories, promising operational efficiencies, sustainability, and environmental considerations. As businesses and stakeholders chart their course into the future, a nuanced understanding and proactive adaptation to these transformative forces become imperative for sustained success.

5.2 Cyber-physical systems

The fourth industrial revolution is increasingly developing cyber-physical systems that innovate industrial engineering and traditional control systems with the deployment of advanced technological paradigms such as IoT, machine learning and artificial, big data with the goal of making factories more efficient and with greater manufacturing innovation with a higher degree of self-awareness and self-configuration. There is currently a push toward the adoption of the Fog Paradigm to improve all engineering applications that reached real-time execution with high reliability, such as minimising communication errors, and toward the cloud for all applications that require high raw computing powers [14].

Developing particular information infrastructure, monitoring, and control strategies intended to retain controllability under external disturbances and unforeseen breakdowns can increase the safety and performance of industrial systems [15].

Security becomes a key worry as these systems become increasingly sophisticated, linked, and connected to physical items. A systematic and organised perspective of security-related data seems necessary for different operations, such as security analysis and creating security controls and architectures [16].

The introduction of these changes involves a phase of adaptation of present systems as particular in engineering applications require a combination of computational power and latency for which it is required to develop both hardware and software sided of cyber-physical systems. Industrial cyber-physics aims to ensure efficiency and performance in line with Industry 4.0 requirements while managing control applications that require real-time decision-making processes. Although cloud interfaces have generally been utilised to facilitate the deployment of cyber-physical systems, there are real limits in terms of consistency, dependability, and external risk factors (such as broadband outages). Although the compute capability of the fog interface is also constrained, these limits might be lessened by inventive design and engineering. On the other hand, the clouds' inconsistency when it comes to real-time performance is not indicative of the topology or architecture that underlies it. Therefore, industrial cyber-physical systems enabling Industry 4.0 engineering applications and scenarios would seem more naturally adapted to the decentralisation, flexibility, and consistency offered by fog computing [14]. Moreover, industry 4.0 saw the introduction of the ICS (industrial control system). In this field cyber-attacks may result in disruptive effects, such as large societal and financial losses and, in fact, it has been presented a communized architectural method from the viewpoints of ICS security-related technologies, ICS cyberthreats, and ICS procedures to proactively handle the security issue of ICSs [17].

A Cyber-Physical System (CPS) [6] consists on combining the physical world and the cyber one. Research has demonstrated the existence of a hardware/software framework that supports run-time resilience for cyber-physical systems, using digital twins, to simulate, control processes, improve safety at work, and failure models to optimize operation, integration, maintenance and recovering ability for various use cases, particularly for contexts such as intelligent cities and industrial IoT [18]. CPS are known for being large, heterogeneous and networked, for their interconnection, complexity. They are systems whose operations are tracked, coordinated, controlled and integrated by components that interact with the physical world through computing, transmission and other means. Unlike traditional stand-alone embedded systems, CPS is based on the networking of multiple devices. That is to say, CPS is a modernised embedded system able to send and receive information through wired or wireless network, enabling on-demand search, access, exploration and/or recovery of information and resources, as well as intelligent analysis, use and linking, allowing anyone to perform automated diagnostics and tasks anywhere, anytime. Cyber-Physical Production Systems (CPPS) are being developed to apply CPS to industrial production systems. CPPS combines a conventional production system and smart equipment, data storage and fast processors. This enables production facilities to communicate, act and manage each other in an independent way thanks to adaptive networks. Thus, it enhances core manufacturing processes when it comes to decentralised decision-making, industrial added value, supply chain and lifecycle management, manufacturing technology and resource consumption. Cyber-physical human-centric (CPHS) has evolved to align with the targets of complex industrial plants to be human-centric, resilient and sustainable [19]. Manufacturing processes based on collaborative robots and large machines allow for improved operator safety and traceability. The proposed use case focuses on a factory floor where human proximity sensing is used to determine when a machine should or should not be running to use resources more efficiently and prevent accidents or incidents involving such machines. A CPHS proposal uses a mixed edge computing structure and intelligent fog computing points that analyse thermal pictures and take industrial safety actions. Experiment results demonstrate that in the chosen real scenario, the algorithm developed for CPHS is capable of quickly and accurately detecting human presence (in less than 10 ms with 97.04% accuracy) using low-powered equipment such as Raspberry Pi 3B and providing an efficient solution (a good trade off among efficiency, robustness, and performance) that could be implemented in many Industry 5.0 applications.

The difficulties of having an ageing crew can also be mitigated by switching from hazardous on-site, in-vehicle labour to remote, computer-assisted piloting, making the job more appealing to new generations, using virtual reality (VR) and augmented reality (AR) for remote control and modern telepresence techniques.

People operating the robot or working in a collaborative application must go through a learning and training procedure for safety concerns. The foundation of intelligent automation is the proficient and effective control of robots and the safety of those robots in industrial settings. Simulators are considered a cost-effective alternative for developing fundamental technical skills and workplace design because many businesses cannot afford to buy a robot expressly for training reasons.

At this stage, process modelling and engagement using virtual reality technology may offer a realistic experience without any actual hazards [20, 21].

The traditional work patterns and protocols used in traditional industries will evolve, update, or completely change with virtualisation of data-driven manufacturing, which enables system-wide communication, coordination, prediction, and control. As a result, resource utilisation is optimised, system performance is improved, production efficiency is increased, product quality is improved, and profitable business development occurs. As a result, there is an increased need for a specifically qualified and trained workforce, which will increase the likelihood that new employment of all kinds will be created.

[6]. Direct video feeds from on-machine cameras can be used by operators with a variety of connection options (5G, wired ethernet), depending on the video compression quality [22, 23]. To build a virtual depiction of physical systems where both components are linked to share data, the idea of "digital twins" has been presented. Emerging Digital Twin technologies are progressively pivotal for comprehending system resilience and identifying risks. Initially, the evolution of digital twins prioritized concerns regarding worker safety by leveraging process modelling and system integration. However, the scope of Digital twins has expanded to encompass diverse realms such as monitoring cash and carbon flows. By employing Digital twins for intricate simulations and analyses, organisations can proactively mitigate risks, optimize operational efficiencies and gain valuable insights into various aspects of their operations. The integration of Digital twins into broader considerations like financial and environmental sustainability signifies their versatile application in enhancing overall system resilience and risk management strategies. However, this broad term covers a number of significant difficulties for the creators of such features. How to give the virtual duplicate a human viewpoint is one of them [24–26].

Therefore, data analysis and artificial intelligence research for intelligent firms became an official trend: they target to analyse raw information to find hidden patterns and linkage between various variables. The growth of data storage, computing power, and analytical algorithms—all of which have seen a rapid advancement—has occurred concurrently with the development of IoT and CPS technologies. Industry 4.0 paves the way for real-time controlling and synchronisation of the physical-virtual link and the networking of CPS components to the virtual realm [27, 28].

The conventional issues with hardware, software, and networked systems are connected, which poses a significant new difficulty. As a result, a comprehensive, systematic investigation of the viability, robustness, performance assessment, and performance optimisation of the ICPS monitoring and control techniques becomes essential [29].

Network security features are crucial for safeguarding important infrastructure. New intelligent network designs are a must to nowadays' industrial control systems, especially the creation of the "Collaborative Robotic Cyber-Physical System" (CRCPS), an industrial security framework for a harmless and secured human–robot cooperation (HRC) in an industrial networked production environment. Industrial clients of "collaborative robot manufacturers" that deal with automatic and semi-automatic manufacturing processes are becoming more and more focused on balancing their manufacturing processes to a level that allows smooth human–robot collaboration. This is especially true for semi-automatic procedures used in the automotive sector but still require human workers to perform some duties manually. The industrial CRCPS's network security is essential since the system's goal is to protect workers using its heavy-payload collaborative robots from potentially fatal situations. Important information inside CRCPS must be secure and cannot be compromised as a result of a malicious attack, in addition to worker safety [30–33].

Intelligent anomaly detection remains a difficult problem, particularly when working with limited labelled data to ensure cyber-physical security. This is necessary for spotting cyber-physical menace for reaching efficient and safe work. A few-shot learning model with a Siamese convolutional neural network (FSL-SCNN) has been proposed by certain studies to address the over-fitting issue and evolve in precision for intelligent anomalies identification in industrial CPS [17].

The dependability characteristics of system components, their interconnections, and the structural and behavioural features of the entire system must all be thoroughly understood to conduct a good analysis of the CPS. Such an investigation of intricately entwined system characteristics poses significant hurdles to the suitable modelling and analytic techniques and applicable software tools [9].

It is necessary to have a general understanding of cybersecurity and its key usage for Industry 4.0. Cybersecurity is a challenging procedure that aids in solving numerous hacking problems of Industry 4.0. The emergence of Industry 4.0 technologies is altering how machines and related data are acquired in order to analyse the information they contain. Cybersecurity is a major concern for Industry 4.0 tools, platforms, and frameworks [34].

The interplay between the physical and virtual worlds also generates dangers that must be managed. For instance, robots and humans both operate in cramped quarters in highly automated industrial systems. Such arrangements put everyone at risk, even those who work there [35].

The goal of fault detection systems in current research and technical paths is to set off alarms to properly notify problems occurrence as well as their deepest root causes. Nevertheless, there's still open questions about how quickly it needs to be fixed and how much fault-tolerance, maintenance, and fault recovery are required. More analyses are required to assess the effect of the discovered flaw on the overall performance of the plant [36].

In practically all industrial sectors, equipment maintenance is a critical issue since it affects any production system's standard, security, and output. Additionally, rescheduling production frequently because of accidental and unanticipated interruptions can take a lot of time, particularly for centrally managed systems [37].

Existing solutions do not yet include the psychological dimensions of safety in the area. This deficiency may result in dangerous circumstances, impairing the functionality of the functioning system [72].

However, the inherent unpredictability of the underlying sensor networks is frequently disregarded. The flexibility and robustness of the production process are improved by constructing several modular Cyber-Physical Systems (CPSs) that function as a whole in manufacturing processes, such as a production line made up of many Collaborative Robots (cobots). Verifying this compositional process while considering uncertainty is still difficult [38, 39].

In fact, heterogeneity, interdependence, complexity, unattended nature, growing machine intelligence, autonomous reconfiguration, and uncertainties challenge a CPS. Uncertain system failure, complicated socio-technical systems, human–machine interfaces, cyber-physical assaults, unprotected remote configuration, a lack of standards, and resilience are among the safety and security problems [40].

Another important aspect are the impacts on environmental and economic sustainability [41].

Industry 4.0 will bring other problems and possibilities for processes safety and environmental protection experts, even though they were consistent pillars in studying the influence of automation on safety. However, in the widest sense, it may be thought that everyone who has a stake in the issue-including business, the environment, and the community is accountable for protecting the environment [42].

5.3 Cyber resilience protection

The trend toward Industry 4.0 compounds risks associated with working in industrial environments. In such dynamic contexts, approaches are required to analyse Safety Communication (SC) [43]. Individual SC averages and quantitative evaluation metrics are the main topics of current investigations. This essay suggests a qualitative method for the SC analysis through which a process chain in an engineering firm may be looked at. The findings show that SC is implemented as a sophisticated network of communication channels [44]. This system's flaws cause various issues when it comes to workplaces and process chains. SC does not adhere to Industry 4.0 standards because of a lack of digitisation. These involve producing digital SC material, enhancing businesses' resistance to new risks, and preparing content for current SC media in accordance with work contexts and related activities [45]. The strategies currently in use, developed for a long time with criteria of reliability and safety, as well as productivity and production quality, appear outdated in the last ten years or so. Global manufacturing operations today have more demanding standards than ever before, including things like transaction security and privacy. Manufacturing control is not a new concept, but the integration of distributed manufacturing facilities and the complete control of the manufacturing processes in these facilities is a current research topic, which is denoted with expressions like virtual factories, cloud manufacturing, industrial 4.0, industrial IIoT, and lately, manufacturing based on software-defined networks (SDN). SDN is a network structure that decouples the network information from the monitoring system in the world of computer networks. According to the requirements of each individual application, the SDN structure attributes all data monitoring to a logically centralised, software-programmable control plane. In terms of security, anyone with a computer running network monitoring software may likely take over your whole network. The integrated modelling environment proposed in this study for SDN applications addresses virtual manufacturing system assurance through cybersecurity and resilience methods [46].

In this regard a Maintenance Management system could be adopted by using machine learning to predict downtime and particularly advanced and winking at Industry 5.0 may be implementing an additional system with Privacy Preserving as its goal using Machine learning systems.

A proposed architecture called PriModChain may be utilised for safe sharing and machine learning in an IIoT environment [47]. The practicality of the framework has been examined based on of privacy, security, dependability, safety, and resilience.

The key technology underpinning Industry 4.0 is industrial cyber-physical systems, which integrate traditional industrial and control engineering with cutting-edge technological paradigms (such as big data, the internet of things, artificial intelligence, and machine learning), to create self-configuring, self-aware firms that can bring significant production advances [48].

Through innovation and revolutions, advancing engineering expertise and knowledge continue to make the world safer while fostering economic growth [49].

The technologies and structures required to link and expand actual manufacturing processes to the online environment have not yet been completely developed. Despite the widespread use of cloud computing and service-oriented structure, these implementations are frequently created from the information technology perspective, which can ignore issues with engineering, control, and Industry 4.0 design related to real-time performance, reliability, or resilience [14]. The Internet of Things (IoT) is a developing networking infrastructure that is gradually tying together embedded systems, which are physical systems that have been enhanced with computers, around the globe.

Traditionally, embedded systems have been focused on using sensors and actuators to regulate a particular phenomenon. They are frequently dedicated to a small group of connected physical items, typically carrying out a straightforward operation or application by a unique controller.

Because of widespread connection, cyber-physical systems (CPS) may be considered an extension of embedded systems [50].

5.4 Human robot relationship

Recent advancements in manufacturing technology, often called Industry 4.0, aim to create intelligent firms with more automated supply networks and manufacturing lines. In this instance, the main idea behind Industry 4.0 (I4.0) is the incorporation of cutting-edge solutions into workplace environments and business processes, which call for paradigms that significantly impact people and technology. Adopting technological innovation benefits businesses because it guarantees major benefits, such as costs, technology, management, etc., and it enables employers to improve employee safety [51].

Although new procedures, innovative technology, different types of workplaces, social or managerial transformation, and the fact that "new scientific understanding permits a long-standing problem to be classified as a risk" are all sources of new emerging risks. One illustration of this is the risk to working conditions posed by new tools that necessitate cutting-edge safety evaluation techniques. As stated by the EU Agency for Safety and Health at Work's expert prognosis on Named Entity Recognition (NER) [52], workers experience more mental and emotional strain due to the difficulty of new pieces of knowledge, the renovation of work methods they cause, and poorly designed human-apparatus boundaries.

However, this important development does not completely merge with the requirement for human workers; at the opposite, it necessitates their participation in a hybrid task-execution process in collaboration with robots. When it comes to future firms integrating humans-robots collaboration by working side by side closely in shared workspaces, creating safe environments for human workers is essential.

Collaborative applications face high risks due to the ambiguity of human behaviour and, subsequently, the actual implementation of operations. Currently, some new technologies can transform the informal and goal-oriented description of a human–robot collaboration application into a logic model, taking into account many important teamwork factors, such as work cell layouts, robot kinematics, operator characteristics, robots-operators interaction in tasks, and their corresponding risk estimates.

Therefore, it is essential for a thorough safety investigation to develop a model seeing humans as more than just an operational element and simulates their mistaken behaviour.

In particular, it is extremely important to concentrate on formal models that replicate the most typical human errors that can happen while carrying out manufacturing tasks; doing so enables the identification (and correction) of random events which might go unnoticed if a completely functional human model is used [53].

These topics are extensively studied everywhere. Under the opening of many small and medium sized enterprises (SMEs) that not only constitute a high potential market for robotics across a variety of industries but face similar challenges in the global market as well, including the need for fast reconfiguration of their manufacturing structures, improved safety, smaller manufacturing runs, and lower expenses.

Usage of developed robots in production systems is, in fact, spreading throughout business. Previously utilised mostly in large, high-tech manufacturing facilities, robots are now more widely used by various manufacturing organisations, including small- and medium-sized enterprises (SMEs) that aren't necessarily involved in the high-tech sector. As a result, workplaces where humans and robots coexist are frequently physically divided, which limits their flexibility and efficiency.

Collaborative robots are typically implemented in common spaces and put through various tests that gauge their effectiveness and performance concerning human safety criteria for robotic systems that can reduce the chances of important low-level injuries [54].

It is important to look into automatic standard compliance to reassure that each component is safe to interoperate. Given sets of security and safety standards are used to create standard compliance, from which quantifiable indicator points are produced. These represent system configurations advised by applicable security, safety, or process management standards and guidelines, helping to show the degree of compliance [55].

The capacity to assemble the pieces and cohabit with robots while studying the ergonomics of the human worker in cramped areas without endangering the worker's safety (for example, in the aeronautical industry) is a key aspect of the human–robot relationship [56].

Industry 4.0's cloud-based idea envisions moving computer numerical control (CNC) operations to the cloud and offering them to industrial equipment as a service. One of the numerous advantages of C-CNC is that it enables machines to use cutting-edge monitoring algorithms working on cloud computers to improve their performance at a cheap expense and avoiding significant hardware modifications [57].

5.5 Workers' safety

The constant adoption of new technologies in the workplace calls for paradigms that significantly impact both people and technology. Adopting technological innovation is beneficial for businesses because it guarantees major benefits, such as those related to technology, efficiency, administration, etc., and it enables employers to improve employee safety. Technological advancements necessitate consideration of risks to workers. Indeed, it is important to highlight new risks of injury, new probable illness sources or hazards caused by innovative operations and procedures.

For instance, new risks for injuries, new probable diseases cause or threats brought on by new practices or activities should all be considered.

This paragraph indicates that there is no comprehensive overview of the unique risks associated with the application of novel solutions in production systems. So, a meticulous analysis was conducted to study various solutions and identify risks associated with the technical solutions under consideration. The implementation of solutions, like IoT, Cloud, and Artificial Intelligence, characterises the industry 4.0 transformation process [51].

These modern technologies may have a great impact on everyday work. However, it is challenging to independently examine every solution' risks for the employees due to the creation of an underpinning level constructed with several innovative solutions, each of which is defined with a variety of features. Workers' health and safety risks are not only related to the abovementioned technologies; rather, they should be examined in light of the particular technological solution used in each situation. For this reason, the study that has been presented has only looked at the technologies that presents a serious threat to the health and safety of workers. In light of this, eight technology categories were established: additive manufacturing, AGV, augmented reality/virtual reality, exoskeleton, robot/cobot, and smart mobile wearable devices.

The risk factors identified for each technology have been categorised according to ISO 12100:2010 (Safety of machinery—General principles for design—Risk assessment and mitigation), and two additional risk sections—Organisational Risks and Psychological Risks—have been integrated to provide a broad set of norms for the context being analysed. Organisational hazards occur when risk is associated with policies, processes, standards and organisational solutions unrelated to the worker's actions. The connection between the worker and digital technologies and their subjective view of their work are the sources of psychological risks. In addition, the risk categories of 12100:2010 have been renamed as follows to provide a broader and more thorough reference in this context: Chemical and biological replaced the category "Materials and substances", while the section "Environment" changed into "Work environment and microclimate" [58].

For example, research shows several sensors to monitor various physical and behavioural biometric parameters. This is made possible by the combination of multiple biometric traits with the assistance of machine learning technologies working in conjunction with various types of sensors [59]. The authors' approach is simple to execute in a large-scale intelligent firm, and experiments employing COTS hardware have demonstrated how it will further the adoption of Industry 4.0.

The authors present evidence that their suggestion can greatly increase operator safety while averting fatal collisions. By using various smart devices, it is possible to gain a thorough understanding of how operators operate and prevent injuries when operating industrial machinery. Industry 4.0 adoption is accelerated by experiments using readily available hardware to show how the concept can be easily implemented in a large-scale smart plant. Additionally, using lightweight approaches shows that multibiometric system integration is possible without high-performance hardware, enabling businesses to keep costs low while implementing these new technologies.

While one among most disruptive phenomenon of the past 20 years, COVID-19 pandemic showed the susceptibility of multinational industrial corporations to their supply networks and operations. It proved that big businesses undervalue the requirement for resilient and sustainable operations. Due to a variety of factors, the pandemic's worldwide impact is enormous for supply chains that are interrupted. For example, Wuhan, the epicentre of the COVID-19 outbreak, is home to numerous large manufacturing firms where suppliers of auto parts and semiconductors to major automakers like General Motors, Hyundai, Toyota, Volkswagen, Honda, etc. are concentrated. Additionally, any disruptions in China and India had an impact on businesses around the world. The effects of disruptive occurrences, such as a shortage of raw materials, delivery delays, a lack of replacement parts, a reduction in labour capacity, etc., directly affect operations. Additionally, [60] created a model to assess how a pandemic might affect the supply chain network and manufacturing resilience. It is clear that COVID-19 event presents a chance to create a flexible and resilient manufacturing system to maintain the organisations' social, environmental, and economic sustainability, focusing more and more on the centrality of the man in order to overcome classical workers' theories and design a more sustainable worker environment [74].

These procedures help the organisation's financial situation. As a result, the best techniques for both socioeconomic development and environmental preservation were merged. The detrimental effects of the tragedy on business operations and industrial policy are causing worry among experts, governments, corporate executives, and legislators. As a result, businesses seek to solve the problems and difficulties related to three components of sustainability. As a result, numerous initiatives have been made to alter businesses, including those that concern employee well-being, effective healthcare communication tactics, workers safety, smart working circumstances, and capability development. These are a few social sustainability programs organisations have implemented to lessen COVID-19's effects and maintain social sustainability.

The management and execution of work tasks has recently undergone a rapid transformation thanks to the introduction of new technology. Building Information Modelling (BIM) is more frequently used to enhance performance of different tasks, particularly in the construction industry. With this in mind, and given that construction industry remains one of the most dangerous workplaces, several studies have suggested that BIM is essential for effectively improving workplace safety. In this perspective, [1] examine contemporary studies on the application of BIM to increase building site security. The study found that design for safety with BIM, dynamic visualisation and feedback had a more legitimate research direction. According to the study's findings, more BIM practices are required, particularly in safety education and training, using BIM to improve the climate and resilience of safety, and creating quantitative risk analysis to better support security management.

A future proposal in the era of the IoT, in industrial settings, sensors, actuators, and smart objects are used to direct all sides and operations of a firm, from standard available systems, such as lighting, production, and automation systems, to crucial systems, such as safety and fire protection systems that detect structural integrity. In crucial and urgent situations, such as wildfires and other disaster-inducing events, it is critical to seek assistance and resources from third parties, particularly nearby entities, in order to respond to the emergency as soon as possible. This also applies to smart services such as fire management and building evacuation, which should be made resilient in the face of similar catastrophic events. As a result, there is an Industry 4.0 initiative where a system can monitor the progression of flames and protect each district area from power outages or disconnections [61].

Industry 4.0 is a notion that has recently emerged as a result of connection and intelligent automation of the Internet of Things. These new technologies should benefit job circumstances, productivity growth, and new company models. Workplace safety is one of the most delicate issues that calls for precise and focused answers. Investigating the workers' attention states, particularly their degrees of sleepiness, can help ensure their safety. Many technologies have used biometrics to address this issue, but how many of them are actually usable in an Industry 4.0 real-world scenario? [62, 63].

Some studies also have shown how the introduction of mobile apps for smartphone can improve the safety level in industry [64], creating an interconnection between multiple machineries and workers [65] while the primary objective being to increase human safety in production systems relying on collaborating robots or other machinery [19].

Every workplace should provide protection for workers' safety throughout routine operations as well as unusual tasks (like maintenance), but the industrial sector is the one where worker dangers are the greatest.

The following are a few instances of the types of abuses or easily predicted human behaviours that must be taken into consideration from the ISO 12100:2010 standard: "(a) loss of control of the machine by the operator; (b) reflex behaviour of a person in case of malfunction, accidents or failure during the common use of the machinery; (c) behaviours resulting from lack of concentration or carelessness; (d) behaviour resulting from adopting the line of least resistance in carrying out a task (e.g., a given machinery is designed with redundant safety devices and, as a consequence, the worker removes/disables the safety devices to work faster thinking that they are not important); (e) behaviour resulting from pressures from the bosses to keep the machinery running in all circumstances; (f) the behaviour of specific kind of people such as children." All of those behaviours are expected in part or in whole during machinery designing, but if the equipment is turned off or in maintenance mode, it is impossible to take the appropriate countermeasures [66, 67].

6 Future developments

While many worldwide factories are still struggling to get along with the principles of Industry 4.0, others are already looking towards the future as they have started the transition to Industry 5.0. Within this concept, Cyber-Physical Human Centred Systems (CPHS) emerged to harness operators' capabilities. To achieve the target of complex production systems, CPHS is based on three salient points: human-centricity, resilience and sustainability [19].

In particular, about human-centricity, was discussed how Lean Thinking can contribute to the 5.0 Society and Industry 5.0. In the area of sustainability, efforts are made not to waste water and raw materials. Human potential that is unrealised is another sort of waste. This waste is a result of operators' suggestions, inventiveness, and original ideas not being capitalised. Now that technology is all around us and encourages creativity more than ever, creative people are even more needed. Technology can also restrict actions and stifle innovation. Because of this, technology adoption must be carefully thought out and justified. When technology is effectively integrated, creativity and the potential of the individual can be completely unlocked [68].

The requirements Industry 5.0 has sparked formal discussions about the need for manufacturing to be human-centric, with the well-being of industry manufacturers at the centre of production systems rather than system-centric, with only efficiency and quality improvement and cost reduction as its driving forces. An "Industrial Human Needs Pyramid" was created to present and classify human needs and motivations in production as a fundamental contribution to the knowledge of workers' needs. (Fig. 8) [69].

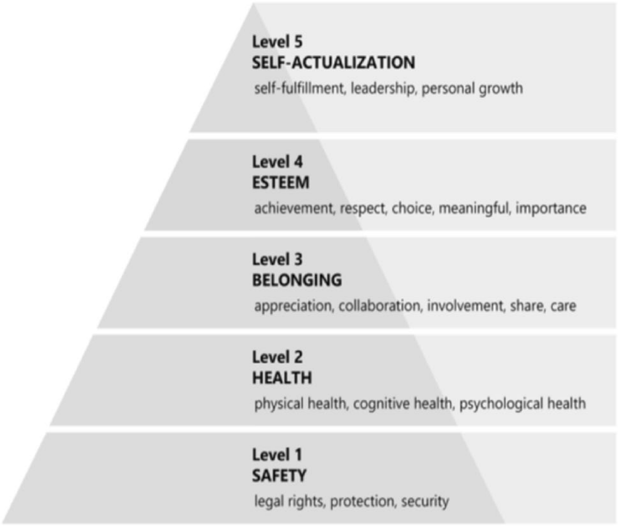
The pyramid's five tiers, starting by the base then the top, depict the evolvement from ensuring fundamental human safety to promoting personal development:

Level 1: Safety. Prior thing an industrial environment should achieve is physical safety. A combination of isolation and reactive machines-humans protection is used in today's protective techniques. Adaptive planning and execution of safe human–machine interactions are required as the protection mechanism must go from reactive protection to proactive protection, where the environment can detect and forecast manufacturers' behaviour.

Level 2: Health. Healthy working conditions are Level 2 needs. Physical health in this step describes a setting that reduces unsafe motions, postures, or working patterns that result in long-term musculoskeletal injury. The production environment must as well offer high-value jobs to promote manufacturer engagement while decreasing cognitive stress to keep manufacturers psychologically healthy.

Level 3: Belonging. This level begins to respond to a worker's social characteristics. Because we are a social species, cooperation is essential for our survival and development. The term "belongingness" describes people's psychological

Fig. 8 Industrial Human Needs Pyramid. [69]



need to connect with others, affiliate with groups, and feel linked. Friendship, intimacy, trust, acceptance, receiving and giving affection, and admiration are some of belonging requirements.

Level 4: Esteem. Esteem needs include self-assurance, courage, conviction in oneself, social and personal acceptance, and respect from others. One of the key steps to obtaining self-actualisation meets these requirements. Although esteem is an internal trait, humans are influenced by outside forces, like peer validation and approval.

Level 5: Self-actualisation. Self-actualisation refers to realising personal potential, seeking personal growth and peak experience. Workers at this level view their job largely as a means of achieving personal fulfilment. They have a feeling of purpose that they naturally incorporate into their daily operations, embrace themselves and others, and maintain deep and lasting relationships.

7 Research proposition

In order to direct future works on industry development, englobing the main elements of this work, the research proposals might be included in the study's conclusion.

RS1: An increase in the centrality of humans in workers' time and location development activities.

RS2: Greater integration of machines and workers, decentralising control and recording every activity according to safety deployments. Shift the load of burdensome and repetitive work to the machine and robot, transforming them into collaborators and helpers of the workers.

RS3: Introduce metaverse work to improve integration between operators in distant locations, unifying companies with distributed locations. Reduce development time and costs with virtual simulations and physical tests extracted from likely working conditions on real components.

Future work demonstrating innovative safety procedures in intelligent industry, where knowledge of the methodologies or epistemologies used by specialists in the field may be considered for experimentation, is yet anticipated. The researchers might also employ the study suggestions for further advancement. [69]

Moreover, by using cyber-physical systems, artificial intelligence, the industrial Internet of Things and combining those technologies, industry professionals might boost the efficacy of the created approaches [70].

8 Conclusion

We are in the era of Industry 4.0, and companies are undergoing a significant structural operational transformation and overcoming many challenges to adapt production in an intelligent and environmentally friendly way to meet the demand for affordable, customised, and high-quality product on a global scale.

The intelligent artefacts can communicate with each other and rearrange and reorganise themselves to produce diverse customised items flexibly and sustainably. Research has shown that responsiveness is the most crucial factor, and that high service levels, expense-cutting, recovery, safety standards, and working conditions are the most crucial criteria for each of their respective elements [71]. Moreover, "Industrial Big data" may be obtained from a sizable number of smart things dispersed geographically and transmitted to the cloud. The "gold" for Industry 4.0 may be in the proper big data analysis and processing. Data-based virtual production enables system-wide coordination, prediction, and monitoring, resulting in greater system performance, increased production efficiency, higher-quality products, lucrative business growth, and more. Therefore, the typical labour patterns and norms used in traditional industries will alter, evolve, or maybe go entirely out of style. As a result, there is an increased need for a specifically skilled and trained workforce, which will increase the likelihood that new jobs of all kinds will be created [3]. This technological process, however, must also be accompanied by an advancement in security.

Indeed, in order to protect the user, future technical advancements should focus on integrating safety systems and systems for detecting workplace and worker circumstances. It should also be mentioned that developing risks include psychological elements in addition to physical and physiological ones. In order to close the gap about employee health and safety, policing terms of specific 4.0 technology adoption, it has been demonstrated how digital innovation within manufacturing systems it can help companies enhance the safety and well-being of manufacturers as well as production. Thus, projecting companies towards the fifth industrial revolution.

Author contributions G.M. Writing and correcting D. M. Writing and correcting N.L. Writing and correcting.

Funding No external funding was used.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

1. Fargnoli M, Lombardi M. Building information modelling (BIM) to enhance occupational safety in construction activities: research trends emerging from one decade of studies. Buildings. 2020;10(6):98. https://doi.org/10.3390/BUILDINGS10060098.
2. Gallab M, Bouloiz H, Kébé AS, Tkiouat M. Opportunities and challenges of the industry 4.0 in industrial companies: a survey on moroccan firms. J Indus Bus Econ. 2021;48:413–39. https://doi.org/10.1007/s40812-021-00190-1.
3. Hsu C-H, Zeng J-Y, Chang A-Y, Cai S-Q. Deploying industry 4.0 enablers to strengthen supply chain resilience to mitigate ripple effects: an empirical study of top relay manufacturer in China. IEEE Access. 2022;10:114829–55. https://doi.org/10.1109/ACCESS.2022.3215620.
4. Di Nardo M. Developing a conceptual framework model of industry 4.0 for industrial management. Indus Eng Manag Syst. 2020;19(3):551–60. https://doi.org/10.7232/iems.2020.19.3.551.
5. Sood SK, Rawat KS, Sharma G. Role of enabling technologies in soft tissue engineering: a systematic literature review. IEEE Eng Manag Rev. 2022;50(4):155–69. https://doi.org/10.1109/EMR.2022.3195923.
6. Sinha D, Roy R. Reviewing cyber-physical system as a part of smart factory in industry 4.0. IEEE Eng Manag Rev. 2020;48(2):103–17. https://doi.org/10.1109/EMR.2020.2992606.
7. Hasan N, Chaudhary K, Alam M. A novel blockchain federated safety-as-a-service scheme for industrial IoT using machine learning. Multimed Tools Appl. 2022;81:36751–80. https://doi.org/10.1007/s11042-022-13503-w.
8. Gurevitch J, Koricheva J, Nakagawa S, Stewart G. Meta-analysis and the science of research synthesis. Nature. 2018;555(7695):175–82. https://doi.org/10.1038/nature25753.
9. Fabarisov T, Yusupova N, Ding K, Morozov A, Janschek K. Model-based stochastic error propagation analysis for cyber-physical systems. Acta Polytechnica Hungarica. 2020;17(8):15–28.

10 Efe A, Isik A. A general view of industry 4.0 revolution from cybersecurity perspective. Int J Intell Syst Appl Eng. 2020;8(1):11–20. https://doi.org/10.18201/ijisae.2020158884.

11 Garcés L, Oquendo F, Nakagawa EY. Software mediators as first-class entities of systems-of-systems software architectures. J Brazilian Comput Soc. 2019. https://doi.org/10.1186/s13173-019-0089-3.

12. Le CH, Le DT, Arey D, Gheorghe P, Chu AM, Duong XB, Nguyen TT, Truong TT, Prakash C, Zhao S-T, Mahmud J, Gao J, Packianather MS. Challenges and conceptual framework to develop heavy-load manipulators for smart factories. Int J Mechatron Appl Mech. 2020;2(8):209–16.

13 Gupta R, Tanwar S, Kumar N, Tyagi S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: a systematic review. Comput Electrical Eng. 2020;86:106717. https://doi.org/10.1016/j.compeleceng.2020.106717.

14. O'Donovan P, Gallagher C, Leahy K, O'Sullivan DTJ. A comparison of fog and cloud computing cyber-physical interfaces for Industry 4.0 real-time embedded machine learning engineering applications. Comput Ind. 2019;110:12–35. https://doi.org/10.1016/j.compind.2019.04.016.

15 Yin S, Rodriguez-Andina JJ, Jiang Y. Real-time monitoring and control of industrial cyberphysical systems: with integrated plant-wide monitoring and control framework. EEE Trans Indus Electron. 2019;13(4):38–47. https://doi.org/10.1109/MIE.2019.2938025.

16 Settanni G, Skopik F, Wurzenberger M, Fiedler R. Countering targeted cyber-physical attacks using anomaly detection in self-adaptive industry 4.0 systems [Abwehr zielgerichteter cyber-physischer Angriffe mittels Anomalie-Erkennung in selbstadaptiven industrie-4.0-systemen]. Elektrotechnik & Informationstechnik. 2018;135(3):278–85. https://doi.org/10.1007/s00502-018-0615-6.

17. Zhou C, Hu B, Shi Y, Tian Y-C, Li X, Zhao Y. A unified architectural approach for cyberattack-resilient industrial control systems. Proc IEEE. 2021;109(4):517–41. https://doi.org/10.1109/JPROC.2020.3034595.
18. Parri J, Patara F, Sampietro S, Vicario E. A framework for model-driven engineering of resilient software-controlled systems. Computing. 2021;103(4):589–612. https://doi.org/10.1007/s00607-020-00841-6.

19 Fraga-Lamas P, Barros D, Lopes SI, Fernández-Caramés TM. Mist and edge computing cyber-physical human-centered systems for industry 5.0: a cost-effective IoT thermal imaging safety system. Sensors. 2022. https://doi.org/10.3390/s22218500.

20. Pérez L, Diez E, Usamentiaga R, García DF. Industrial robot control and operator training using virtual reality interfaces. Comput Ind. 2019;109:114–20. https://doi.org/10.1016/j.compind.2019.05.001.
21. König A, Thongpull K. Lab-on-spoon - A 3-D integrated hand-held multi-sensor system for low-cost food quality, safety, and processing monitoring in assisted-living systems. J Sensors Sensor Syst. 2015;4(1):63–75. https://doi.org/10.5194/jsss-4-63-2015.

22. Dima E, Sjöström M. Camera and lidar-based view generation for augmented remote operation in mining applications. IEEE Access. 2021;9:82199–212. https://doi.org/10.1109/ACCESS.2021.3086894.

23 Al-Jaroodi J, Mohamed N, Jawhar I. A service-oriented middleware framework for manufacturing industry 4.0. ACM SIGBED Rev. 2018;15(5):29–36. https://doi.org/10.1145/3292384.3292389.

24. Lago Alvarez A, Mohammed WM, Vu T, Ahmadi S, Martinez Lastra JL. Enhancing digital twins of semi-automatic production lines by digitizing operator skills. Appl Sci. 2023. https://doi.org/10.3390/app13031637.

25 Akanmu AA, Anumba CJ, Ogunseiju OO. Towards next generation cyber-physical systems and digital twins for construction. J Inf Technol Constr. 2021;26:505–25. https://doi.org/10.36680/j.itcon.2021.027.

26. Suhail S, Malik SUR, Jurdak R, Hussain R, Matulevičius R, Svetinovic D. Towards situational aware cyber-physical systems: a security-enhancing use case of blockchain-based digital twins. Comput Ind. 2022;141: 103699. https://doi.org/10.1016/j.compind.2022.103699.

27. Fumagalli L, Cattaneo L, Roda I, Macchi M, Rondi M. Data-driven CBM tool for risk-informed decision-making in an electric arc furnace. Int J Adv Manuf Technol. 2019;105(1–4):595–608. https://doi.org/10.1007/s00170-019-04189-w.

28. Cimino C, Negri E, Fumagalli L. Review of digital twin applications in manufacturing. Comput Indus. 2019. https://doi.org/10.1016/j.compind.2019.103130.

29. Jiang Y, Yin S, Kaynak O. Performance supervised plant-wide process monitoring in industry 4.0: a roadmap. IEEE Open J Indus Electron Soc. 2021;2:21–35. https://doi.org/10.1109/OJIES.2020.3046044.

30. Khalid A, Kirisci P, Khan ZH, Ghrairi Z, Thoben K-D, Pannek J. Security framework for industrial collaborative robotic cyber-physical systems. Comput Ind. 2018;97:132–45. https://doi.org/10.1016/j.compind.2018.02.009.

31. Hasan MZ, Ahammed R. Application of Industry 4.0 in LPG condition monitoring and emergency systems using IoT approach. World J Eng. 2021;18(6):971–84. https://doi.org/10.1108/WJE-06-2020-0218.

32. Liu K, Wang M, Ma R, Zhang Z, Wei Q. Detection and localisation of cyber-attacks on water treatment systems: an entropy-based approach frontiers of information technology and electronic. Engineering. 2022;23(4):587–603. https://doi.org/10.1631/FITEE.2000546.

33. Riel A, Kreiner C, Macher G, Messnarz R. Integrated design for tackling safety and security challenges of smart products and digital manufacturing. CIRP Ann. 2017;66(1):177–80. https://doi.org/10.1016/j.cirp.2017.04.037.

34 Haleem A, Javaid M, Singh RP, Rab S, Suman R. Perspectives of cybersecurity for ameliorative Industry 4.0 era: a review-based framework. Indus Robot. 2022;49(3):582–97. https://doi.org/10.1108/IR-10-2021-0243.

35. Börcsök J, Hafiz MI, Alsuleiman A, Schwarz M, Abdelawwad M. Safe position detection based on safety system-on-chip (SSOC) for wireless IoT application. Int J Circuits Syst Signal Process. 2020;1:1.

36. Jiang Y, Yin S, Kaynak O. Data-driven monitoring and safety control of industrial cyber-physical systems: basics and beyond. IEEE Access. 2018;6:47374–84. https://doi.org/10.1109/ACCESS.2018.2866403.

37 Converso G, Gallo M, Murino T, Vespoli S. Predicting failure probability in industry 4.0 production systems: a workload-based prognostic model for maintenance planning. Appl Sci. 2023. https://doi.org/10.3390/app13031938.

38. Xin X, Keoh SL, Sevegnani M, Saerbeck M, Khoo TP. Adaptive model verification for modularised industry 4.0 applications. IEEE Access. 2022;10:125353–64. https://doi.org/10.1109/ACCESS.2022.3225399.

39. Lamrani I, Banerjee A, Gupta SKS. Operational data-driven feedback for safety evaluation of agent-based cyber-physical systems. IEEE Trans Industr Inf. 2021;17(5):3367–78. https://doi.org/10.1109/TII.2020.3009985.

40. El-Kady AH, Halim S, El-Halwagi MM, Khan F. Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Saf Environ Prot. 2023;173:384–413. https://doi.org/10.1016/j.psep.2023.03.012.

41. Balasubramanian S, Shukla V, Islam N, Manghat S. Construction industry 4.0 and sustainability: an enabling framework. EEE Trans Eng Manag. 2021;71:1–19.

42 Junior JA, Busso CM, Gobbo SC, Carreão H. Making the links among environmental protection, process safety, and industry 4.0. Process Safety Environ Protect. 2018;117:372–82. https://doi.org/10.1016/j.psep.2018.05.017.

43. Digmayer C, Jakobs E-M. Analysing safety communication in industrial contexts. J Tech Writ Commun. 2022;52(3):251–90. https://doi.org/10.1177/00472816211014126.

44. Lackorzynski T, Garten G, Huster JS, Kopsell S, Hartig H. Enabling and optimising MACsec for industrial environments. IEEE Trans Industr Inf. 2021;17(11):7599–606. https://doi.org/10.1109/TII.2020.3040966.

45. Lu Y, Ding E-J, Du J, Chen G-C, Zheng Y. Safety detection approach in industrial equipment based on RSSD with adaptive parameter optimisation algorithm. Safety Sci. 2020. https://doi.org/10.1016/j.ssci.2020.104605.

46. Babiceanu RF, Seker R. Cyber resilience protection for industrial internet of things: a software-defined networking approach. Comput Ind. 2019;104:47–58. https://doi.org/10.1016/j.compind.2018.10.004.

47. Arachchige PCM, Bertok P, Khalil I, Liu D, Camtepe S, Atiquzzaman M. A trustworthy privacy preserving framework for machine learning in industrial IoT systems. IEEE Trans Industr Inf. 2020;16(9):6092–102. https://doi.org/10.1109/TII.2020.2974555.

48. Zhou J, Li L, Vajdi A, Zhou X, Wu Z. Temperature-constrained reliability optimisation of industrial cyber-physical systems using machine learning and feedback control. IEEE Trans Autom Sci Eng. 2023;20(1):20–31. https://doi.org/10.1109/TASE.2021.3062408.

49 Vrana J, Singh R. Cyber-physical loops as drivers of value creation in NDE 4.0. J Non Destr Evaluat. 2021. https://doi.org/10.1007/s10921-021-00793-7.

50. Pazzi L, Pellicciari M. From the internet of things to cyber-physical systems: the holonic perspective. Proc Manuf. 2017;11:989–95. https://doi.org/10.1016/j.promfg.2017.07.204.

51 Bertoncel T, Meško M. Early warning systems in industry 4.0: a bibliometric and topic analysis. Int J E-Serv Mob Appl. 2019;11(2):56–70.

52 Adriaensen A, Decré W, Pintelon L. Can complexity-thinking methods contribute to improving occupational safety in industry 4.0? A review of safety analysis methods and their concepts. Safety. 2019. https://doi.org/10.3390/safety5040065.

53. Askarpour M, Mandrioli D, Rossi M, Vicentini F. Formal model of human erroneous behavior for safety analysis in collaborative robotics. Robot Computer-Integr Manuf. 2019;57:465–76. https://doi.org/10.1016/j.rcim.2019.01.001.

54. Dede G, Mitropoulou P, Nikolaidou M, Kamalakis T, Michalakelis C. Safety requirements for symbiotic human–robot collaboration systems in smart factories: a pairwise comparison approach to explore requirements dependencies. Requirements Eng. 2021;26(1):115–41. https://doi.org/10.1007/s00766-020-00337-x.

55 Bicaku A, Schmittner C, Rottmann P, Tauber M, Delsing J. Security safety and organisational standard compliance in cyber physical systems. Info Commun J. 2019;11(1):2–9. https://doi.org/10.36244/icj.2019.1.1.
56. Ottogalli K, Rosquete D, Rojo J, Amundarain A, María Rodríguez J, Borro D. Virtual reality simulation of human-robot coexistence for an aircraft final assembly line: process evaluation and ergonomics assessment. Int J Comput Integr Manuf. 2021;34(9):975–95. https://doi.org/10.1080/0951192X.2021.1946855.
57. Okwudire CE, Lu X, Kumaravelu G, Madhyastha H. A three-tier redundant architecture for safe and reliable cloud-based CNC over public internet networks. Robot Computer-Integr Manuf. 2020. https://doi.org/10.1016/j.rcim.2019.101880.
58 Costantino F, Falegnami A, Fedele L, Bernabei M, Stabile S, Bentivenga R. New and emerging hazards for health and safety within digitalised manufacturing systems. Sustainability. 2021. https://doi.org/10.3390/su131910948.
59. Abate AF, Cimmino L, Cuomo I, Nardo MD, Murino T. On the impact of multimodal and multisensor biometrics in smart factories. IEEE Trans Industr Inf. 2022;18(12):9092–100. https://doi.org/10.1109/TII.2022.3178376.
60 Eldem B, Kluczek A, Bagiński J. The COVID-19 impact on supply chain operations of automotive industry: a case study of sustainability 4.0 based on sense–adapt–transform framework. Sustainability. 2022. https://doi.org/10.3390/su14105855.
61. Tricomi G, Scaffidi C, Merlino G, Longo F, Puliafito A, Distefano S. A resilient fire protection system for software-defined factories. IEEE Internet Things J. 2023;10(4):3151–64. https://doi.org/10.1109/JIOT.2021.3127387.
62 Bisogni C, Hao F, Loia V, Narducci F. Drowsiness detection in the era of industry 4.0: are we ready? IEEE Trans Indus Inform. 2022;18(12):9083–91. https://doi.org/10.1109/TII.2022.3173004.
63. Shahin M, Chen FF, Hosseinzadeh A, Khodadadi Koodiani H, Bouzary H, Shahin A. Enhanced safety implementation in 5S + 1 via object detection algorithms. Int J Adv Manuf Technol. 2023;125(7–8):3701–21. https://doi.org/10.1007/s00170-023-10970-9.
64. Shamim Kaiser M, Mahmud M, Noor MBT, Zenia NZ, Mamun SA, Abir Mahmud KM, Azad S, Manjunath Aradhya VN, Stephan P, Stephan T, Kannan R, Hanif M, Sharmeen T, Chen T, Hussain A. IWorksafe: towards healthy workplaces during COVID-19 with an intelligent phealth app for industrial settings. IEEE Access. 2021;9:13814–28. https://doi.org/10.1109/ACCESS.2021.3050193.
65. Tomar B, Kumar N, Sreejeth M. Real time automation and ratio control using PLC & SCADA in industry 40. Comput Syst Sci Eng. 2023;45(2):1495–516. https://doi.org/10.32604/csse.2023.030635.
66 Montanaro T, Sergi I, Stefanizzi I, Landi L, Di Donato L, Patrono L. IoT-aware architecture to guarantee safety of maintenance operators in industrial plants. Appl Syst Innov. 2023. https://doi.org/10.3390/asi6020046.
67. Yadav VS, Singh AR, Raut RD, Mangla SK, Luthra S, Kumar A. Exploring the application of Industry 4.0 technologies in the agricultural food supply chain: a systematic literature review. Comput Indus Eng. 2022. https://doi.org/10.1016/j.cie.2022.108304.
68. Alves AC. Lean thinking: an essential mindset. IEEE Eng Manage Rev. 2022;50(4):127–33. https://doi.org/10.1109/EMR.2022.3215062.
69. Lu Y, Zheng H, Chand S, Xia W, Liu Z, Xu X, Wang L, Qin Z, Bao J. Outlook on human-centric manufacturing towards Industry 5.0. J Manuf Syst. 2022;62:612–27. https://doi.org/10.1016/j.jmsy.2022.02.001.
70 Tripathi V, Chattopadhyaya S, Mukhopadhyay AK, Sharma S, Li C, Di Bona G. A sustainable methodology using lean and smart manufacturing for the cleaner production of shop floor management in industry 4.0. Mathematics. 2022. https://doi.org/10.3390/math10030347.
71 Nayeri S, Sazvar Z, Heydari J. Towards a responsive supply chain based on the industry 5.0 dimensions: a novel decision-making method. Expert Syst Appl. 2023. https://doi.org/10.1016/j.eswa.2022.119267.
72 Islam SOB, Lughmani WA, Qureshi WS, Khalid A. A connective framework to minimise the anxiety of collaborative cyber-physical system. Int J Comput Integr Manuf. 2023. https://doi.org/10.1080/0951192X.2022.2163294.
73. Petersen K, Feldt R, Mujtaba S, Mattsson M. Systematic mapping studies in software engineering. In: Proceedings of the 12th international conference on evaluation and assessment in software engineering. EASE'08, pp. 68–77. BCS Learning & Development Ltd., 2008.
74 Durand JP. Creating the new worker: work, consumption, and subordination. Sage J. 2020. https://doi.org/10.1177/0950017020926439.