Solid Freeform Fabrication 2023: Proceedings of the 34th Annual International Solid Freeform Fabrication Symposium – An Additive Manufacturing Conference
Reviewed Paper

State-of-the-art Cyber-enabled Physical and Digital Systems Deployed in Distributed Digital Factory Using Additive and Subtractive Manufacturing Systems: Open, Scalable, and Secure Framework

Ranjit Joy [1], Sung-Heng Wu [1], Usman Tariq [1], Muhammad Arif Mahmood [2 *], Sriram Praneeth Isanaka [1], Asad Waqar Malik [2], Frank Liou [1]

[1] Department of Mechanical and Aerospace Engineering, Missouri University of Science and Technology, Rolla, MO 65409, USA.

[2] Intelligent Systems Center, Missouri University of Science and Technology, Rolla, MO 65409, USA.

[*] Corresponding author – Email: mmahmood@mst.edu, Telephone: +1-573-341-4908, Fax: +1-573-341-4546, Address: Intelligent Systems Center, Missouri University of Science and Technology, 306 Engineering Research Lab, 500 West 16th Street, Rolla, MO, 65409, USA.

Abstract

A distributed digital factory (DDF) integrates physical and digital systems, leveraging additive manufacturing (AM) and subtractive manufacturing (SM), to enable the dispersed production of components. Existing work focuses on digital twins, AM and SM systems, and some security aspects. Nevertheless, a holistic view of integrating devices with dynamic provisions to invoke digital twins has limited supporting research. This paper will detail cyber-physical and digital systems deployed in DDFs. The components of cyber systems, including AM & SM equipment, sensors, communication protocols, and monitoring software, are covered. Challenges associated with the design and deployment of DDFs, such as security, scalability, and interoperability, are detailed. The assessment emphasizes an open framework for DDF development, allowing system integration from vendors & participants across diverse locations and capabilities. The article also examines the significance of a scalable and secure framework for the implementation of DDFs, which ensures the dependability and availability of on-demand manufacturing.

Keywords: Secure distributed digital factory; Additive manufacturing; Subtractive manufacturing; Challenges with distributed digital factory; Scalability and interoperability.

1 Introduction

A digital factory (DF) is a modern manufacturing facility that optimizes and streamlines production processes by utilizing advanced digital technologies such as the Internet of Things (IoT), artificial intelligence and machine learning (AI/ML), digital twins (DTs), automation, and robotics [1]. As shown in Fig. 1, they use digital technology to create a virtual replica of the manufacturing environment, allowing manufacturers to simulate and test production processes before implementing them in the real world [2]. This improves manufacturing efficiency, quality, flexibility, cost savings, and sustainability. DFs are significant as they assist manufacturers in producing high-quality products in a more efficient manner [3]. DFs can reduce the time to manufacture products, increase production capacity, and lower production costs by automating repetitive tasks and optimizing production processes [3]. Furthermore, DFs can monitor production processes in real time, identifying and correcting any problems as they occur, resulting in higher product quality and lower defect rates [4]. DFs also provide manufacturers with flexibility, allowing them to reconfigure production processes quickly in response to changes in product design or demand [5]. It is useful in industries with rapidly changing trends and customer preferences. In terms of cost savings, DFs aid in the elimination of waste and the optimization of production processes, resulting in lower production costs and higher profitability [5].

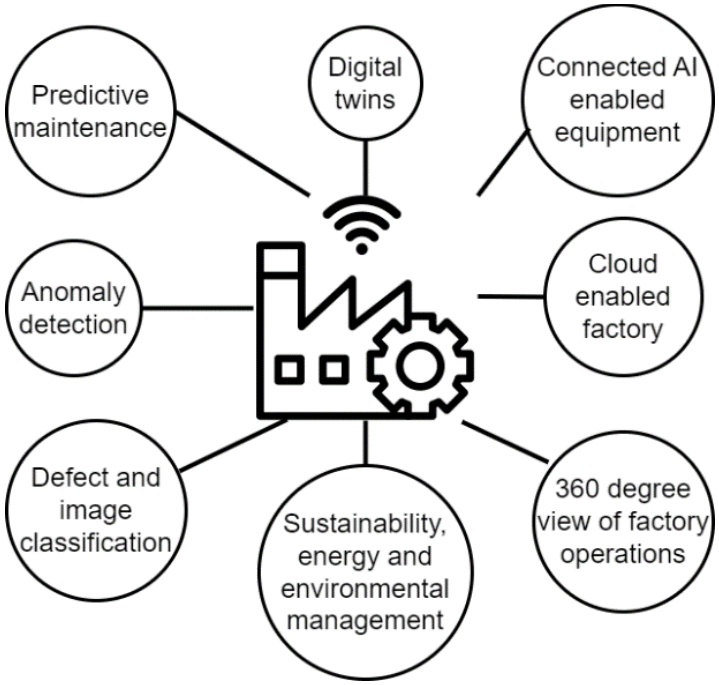

Figure 1. Schematic of a digital factory; based on the information in Ref. [6].

In DF, the convergence of digital manufacturing technologies across every phase of a product's lifecycle is affecting the physical machines on the production floor, encouraged by breakthroughs in manufacturing plant hardware and software solutions [7]. The ability to securely and easily access, transmit, and evaluate real-time streaming data from production machine tools to central IT systems is critical to understanding this amalgamation [8]. While many modern machine tools have sensing and control systems, their data transfer and digital interfaces are usually complex and/or proprietary. The lack of plug-and-play digital integration impedes these equipment's seamless digital operation within DF. Although new CNC machines include MT-CONNECT support, many previous generations require hardware devices as well as particular programming to convert data to the MT-CONNECT standard [9]. When machines on a shop floor are interconnected and integrated into an IT system, insights can be generated to conduct shopfloor and enterprise-level analytics. In turn, such analytics can serve to illuminate both engineering and business decisions.

In DF, the customary procedure for realizing a product comprises four stages: (a) comprehending customer requirements, (b) formulating new ideas, (c) selecting a fitting design proposal, and (d) manufacturing [10], as shown in Fig. 2. The exchange of information among diverse stakeholders, including users, designers, and manufacturers involved in these stages of the product realization process, is crucial for proficient product development [11]. The Internet and other related innovations in IT have supported collaborative design platforms, such as computer-aided design/ computer-aided manufacturing (CAD/CAM) design and process planning, with real-time information flows among stakeholders [12]. This has resulted in the effective assimilation of distributed domain expertise of the stakeholders into the product realization process. Emerging trends in sensing equipment, tracking systems, and location-based services are providing designers with instantaneous information on the product's usage patterns, performance, and failures [13]. The real-time data, coupled with big data analytics, cloud computing, and AI/ML, are providing designers with invaluable insights into their products and users. These advancements are revolutionizing the product landscape by effectively integrating the four stages of the product realization process.

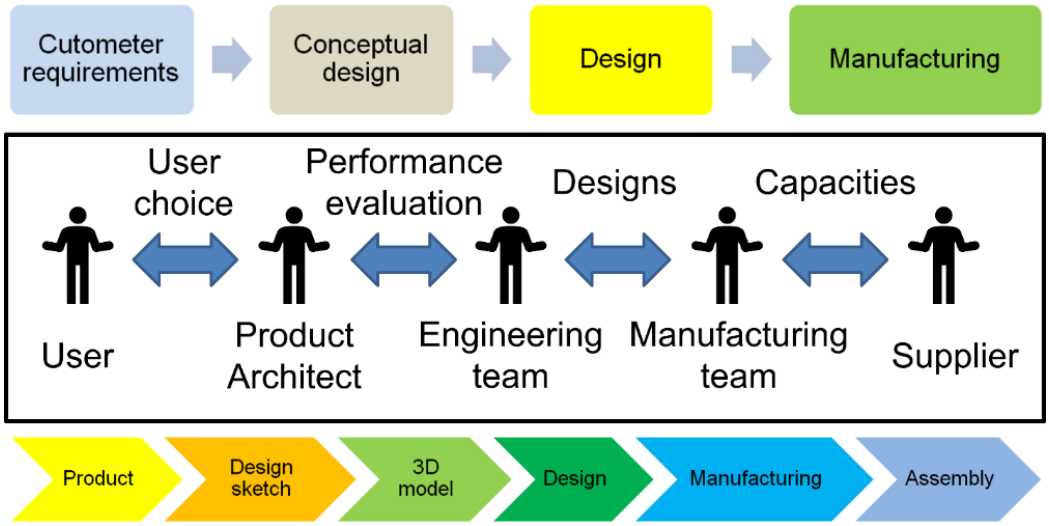

Figure 2. Various stages for a product realization in a DF; based on the data provided in Refs. [10,14,15].

Due to advances in Internet technologies, collaborations in product design and manufacturing are no longer restricted to enterprises and national borders. For effective product development, sharing sensitive information such as intellectual property, business intelligence, and customer information with other collaborators is essential. Due to differences in security practices, laws and regulations, and threat landscapes, these collaborations unfortunately heighten the risk of information leakage. Such variances pose a significant threat to all parties involved in the product realization process, including designers, manufacturers, suppliers, and end-users. In 2013 and 2014, Target's data breach resulted in the compromise of up to 70 million customers' credit card accounts via a third-party vendor [16]. Chrysler announced in July 2015 that it is issuing a formal recall for 1,400,000 vehicles that may be affected by a software vulnerability in the Uconnect dashboard computers due to the threat of hackers [17]. These attacks exploit the system's vulnerabilities and can cause even greater destruction in each system. Individual systems are vulnerable not only to security flaws but also to flaws in the interconnections between these systems, making it more difficult for stakeholders to detect or prevent an attack. In the event of an attack, a vulnerable system that controls physical systems can cause significant damage that extends beyond brand and business operations [18].

These breaches can potentially cause infrastructure damage, negative environmental effects, and even loss of life. Stealth attacks are actions taken by an attacker to conceal their activities to avoid detection [19]. Even after they are launched, such attacks can go undetected. For example, the most well-known stealth attack is Operation Aurora, which targeted thirty-four organizations, including Google and Yahoo, and went unnoticed for more than six months after it was launched [20]. Stealth attacks last an average of three hundred and twelve days before the targeted organization becomes aware of the vulnerability that led to the attack [21]. In some cases, compromised products can be used to provide the computational resources required to carry out such attacks without the users' knowledge. Such circumstances raise ethical concerns for stakeholders involved in the product development process, particularly non-security experts who may unwittingly become targets or participants in an attack. To avoid security breaches, product designers should make security an integral part of the product development process rather than an afterthought.

This review paper introduces the novel concept of distributed DF (DDF) in section 2. Various examples of cyber-physical systems and their DTs have been compiled in section 3 while cyber-physical- and -digital Systems for distributed DF components have been listed in section 4. Section 5 discusses the security considerations and mitigations in DDF. Open standards for DDF have been compiled in section 6. DTs and their development have been highlighted in section 7. The future research directions as well as conclusions have been provided in sections 8 and 9, respectively.

2 Why Distributed Digital Factory is Novel?

A distributed digital factory (DDF) is a manufacturing system that decentralizes and distributes various production processes across multiple locations by utilizing digital technologies and interconnected systems. It enables a network of interconnected manufacturing facilities or nodes by leveraging the power of advanced technologies such as IoT, cloud computing, AI/ML, and automation. An example of a DDF for manufacturing is shown in Fig. 3. Different stages of the manufacturing process can be performed at multiple locations, which are often geographically dispersed, in a DDF. Traditional factory floors, remote facilities, supplier sites, and even customer premises can be considered. The nodes are linked together by a digital network, which allows for real-time communication, data sharing, and coordination. A DDF's key components and features may include (a) connectivity and IoT, (b) data analytics and AI, (c) cloud computing, (d) virtualization and simulation, (e) automation and robotics, and (f) collaborative tools and communication. In connectivity and IoT, the use of sensors, devices, and connectivity infrastructure to collect and transmit data from various machines and equipment in real-time [22]. Advanced analytics techniques and AI algorithms are used in data analytics to analyze data generated by different nodes, enabling predictive maintenance, process optimization, and decision-making [23]. Cloud computing refers to the use of centralized cloud-based platforms to store, process, and share data, thereby providing scalability, flexibility, and accessibility to various stakeholders across the network [24]. Virtual models and simulations are used to test and optimize manufacturing processes, reducing the need for physical prototypes, and lowering the risk of errors or failures [25]. Automation and robotics integrate automated systems, robotics, and autonomous machines to perform tasks with precision and efficiency, reducing the need for manual labor and increasing productivity [26]. Collaborative tools and communication include digital collaboration tools that facilitate communication and coordination among geographically dispersed teams, such as video conferencing, instant messaging, and virtual reality [27].

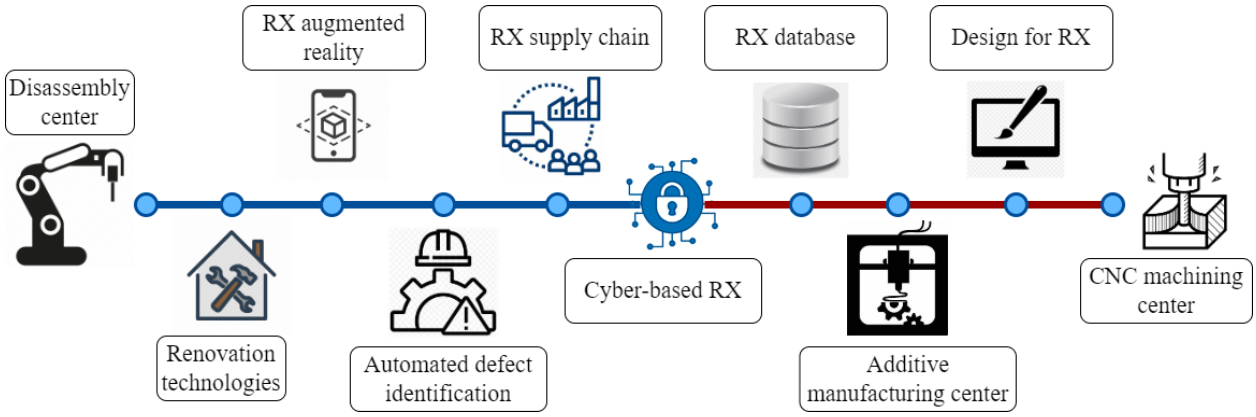

Figure 3. Schematic of a distributed digital factory for manufacturing.

The DDF concept expands on the DF concept by adding a layer of decentralization and distribution of manufacturing processes. A DF focuses on digitizing and optimizing operations in a single location, whereas a DDF goes a step further by leveraging interconnected systems across multiple locations. Production processes in a traditional DF are typically concentrated in a single location [28]. A DDF, on the other hand, spreads production activities across multiple locations, which could include multiple factory sites, supplier facilities, or even customer premises. This decentralization enables greater adaptability and agility in meeting market demands and optimizing resources. A DDF is comprised of interconnected nodes that communicate, share data, and collaborate in real time. This interconnectedness allows for seamless coordination between different locations, data-driven decision-making, and efficient resource allocation and optimization. The DDF concept encourages collaboration and partnership among various manufacturing ecosystem stakeholders. It promotes the incorporation of suppliers, customers, and other partners into the manufacturing process, allowing for shared information, synchronized production planning, and effective supply chain management. A DDF improves scalability and resilience by distributing production processes across multiple locations. It enables easier expansion or contraction of

production capacities based on market conditions, reduces risks associated with single-location reliance, and allows for rapid adaptation to disruptions or changes in demand. Industries can use the DDF to access specialized capabilities or resources located in different locations. Certain regions, for example, may have specialized expertise, better access to raw materials, or lower costs. Industries can improve production efficiency and cut costs by leveraging these distributed resources. The DDF concept represents a step forward in manufacturing operations, leveraging the power of digital technologies and interconnectedness to create a flexible, collaborative, and resilient manufacturing ecosystem. It broadens the possibilities beyond a single location and enables businesses to adapt and thrive in a globally interconnected and dynamic marketplace.

DDF presents several communication and coordination challenges. Effective communication and coordination become more difficult when multiple locations are involved in the manufacturing process. Coordinating tasks, sharing information, and maintaining synchronization between different locations can be difficult and time-consuming. Managing a DDF entails managing a more complex network of interconnected facilities and systems, which adds to the complexity. This complexity can result in increased maintenance and operational costs. Furthermore, managing and troubleshooting technical issues across multiple locations can be time-consuming and challenging. DDF entails the transmission of sensitive data and information across multiple locations and networks, posing data security and privacy risks. This raises the possibility of data breaches, cyber-attacks, and unauthorized access to sensitive information. Implementing strong security measures and protecting data privacy becomes critical, but it can be more difficult in a distributed environment. Setting up and maintaining the infrastructure required for DDF is time-consuming and demands additional resources. To ensure smooth operations, each location must have appropriate technology, connectivity, and supporting systems. This can entail significant upfront and ongoing costs. DDF is heavily reliant on reliable and fast network connectivity. Any network disruption or downtime can impede communication, data transfer, and real-time collaboration between different locations. Because of this reliance on network connectivity, there is a potential point of failure that necessitates backup plans or redundant systems to mitigate the risk. Operating a DDF frequently entails managing diverse teams in multiple locations, which presents cultural and organizational challenges. Collaboration and coordination can be hampered by cultural differences, language barriers, and disparities in work practices. Building a cohesive and unified organizational culture becomes critical, but it can be difficult when teams are dispersed geographically. DDF manufacturing processes may need to comply with various regulatory frameworks and legal requirements in different locations. Navigating complex regulations, standards, and compliance obligations can be time-consuming and difficult.

3 Cyber-physical Systems & Digital Twins

The proliferation of pervasive computing and sensing technologies has aided in the emergence and advancement of cyber-physical systems (CPSs) and Digital Twins (DTs). The evolution of both concepts is defined below.

3.1 Advancement of Cyber-physical Systems and Digital Twins

Due to the interaction between developing technologies and the ever-increasing needs of modern society, cyber-physical systems (CPSs) have undergone a remarkable evolution since their inception. CPS is based on the idea that computers and physical systems can be combined in a single system to improve communication and coordination between the digital and physical realms [29]. A schematic of CPS is presented in Fig. 4. Transformative applications in fields as diverse as transportation, healthcare, manufacturing, and energy systems have resulted from this integration [30].

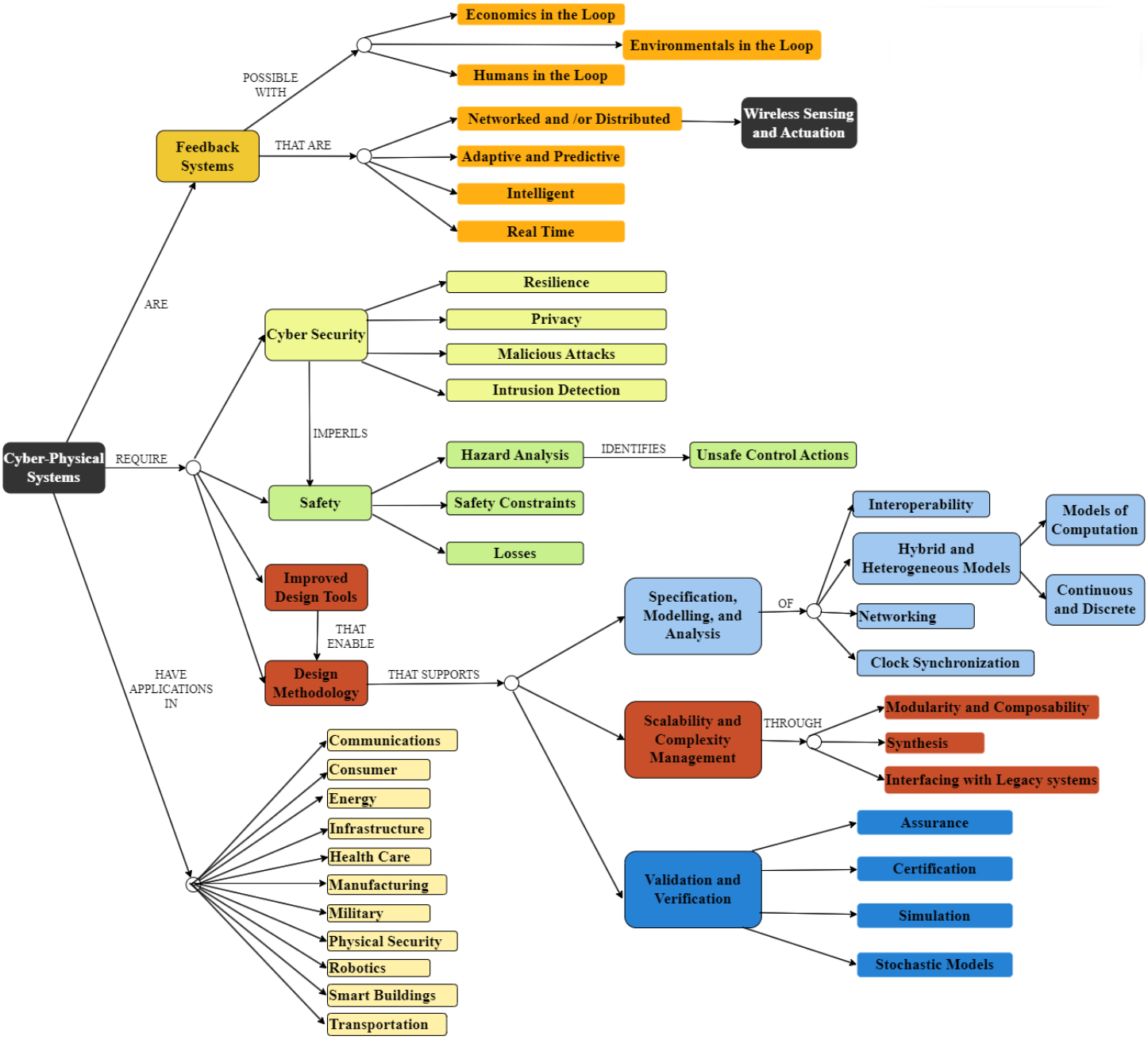

Figure 4. Schematic of a cyber-physical system; based on the information provided in Ref. [31].

Early in the history of computing, disconnected computational systems began interacting with physical processes, marking the beginning of what would later become known as CPS [32]. At first, the focus of such systems was on monitoring and control, using sensors and actuators to track and manipulate physical processes. Networking technologies have gradually made it easier for CPS components to communicate with one another, allowing for remote monitoring and control of dispersed systems [33]. CPS started behaving more autonomously and intelligently as computer device capabilities and miniaturization improved [34]. CPS were given the ability to learn and adapt on their own by the incorporation of AI techniques. As a result, intelligent CPS was developed, which can make decisions and optimize itself in real time based on data, environmental feedback, and set goals [34]. The introduction of IoT has also marked a watershed moment in the development of CPS [35]. By linking devices and sensors, the IoT has enabled the creation of a large network of interconnected physical objects, vastly increasing the scale and scope of CPS [35]. This connectivity has allowed for the unhindered flow of data between

CPS nodes, improving the effectiveness of information sharing and opening the door to novel uses in areas as diverse as smart homes, smart cities, and precision agriculture. Additionally, developments in wireless communication technology have been critical to CPS's development [36]. The shift from hardwired to wireless connections has liberated CPS, allowing for more versatile deployment and more portability [36]. As a result, CPS has been able to spread into more dynamic and mobile settings, such as self-driving cars, wearable tech, and unmanned aerial systems [37]. The current integration of CPS with new technologies such as edge computing and 5G networks has accelerated its development [28]. To reduce latency and provide real-time processing and decision-making, edge computing makes use of distributed computing resources situated closer to the physical systems [28]. Meanwhile, 5G networks' high speed and low latency have opened new opportunities for CPS deployment by allowing the seamless integration of various components across wide geographical areas [38]. The development of CPS has tremendous potential. CPS design and operation may be drastically altered by the advent of quantum computing and its ability to address intricate optimization and simulation challenges [39]. Collaborative CPS, in which humans and machines work together synergistically to increase productivity and expand human capabilities, will also be propelled by developments in robotics and human-machine interaction [40].

Quantum computing could have a huge effect on DTs. A tremendous advancement, driven by the synergistic integration of state-of-the-art scientific fields and cutting-edge technology, has defined the development of DTs) [41]. DTs have progressed far from their original conception as virtual reproductions of tangible assets to complex CPs. The IoT, data science, and AI/ML are just a few of the scientific disciplines that have come together to fuel this shift [42]. DTs can imitate and emulate the complex behavior, performance, and interdependencies of physical things with a new level of fidelity by leveraging cutting-edge algorithms and real-time data streams [43]. The predictive power of DTs has been greatly improved using sophisticated modeling techniques, including computational fluid dynamics, finite element analysis, and multi-physics simulations [44]. Accurate bottlenecks, vulnerabilities, and optimization possibilities can be found with the help of these models for complex procedures, processes, and systems [44]. In addition, dispersed networks have been made possible because of the effective combination of DTs, edge computing, and cloud computing, enabling real-time monitoring, control, and decision-making across a wide variety of networked devices and platforms [45]. Emerging technologies have accelerated the development of DTs. With the advent of 5G networks and their high bandwidth and low latency, DTs have entered a new era of rapid and reliable data transmission between real-world assets and their digital equivalents [46]. As a result, operational efficiency, downtime, and performance may all be boosted across a wide range of domains owing to real-time analytics and decision-making [46]. Quantum computing could have a huge effect on DTs [47]. DTs employ complicated algorithms and models; quantum computing's amazing processing capacity and ability to process huge quantities of data in parallel hold promise for process optimization [47]. This has the potential to open new methods for dealing with difficult optimization problems, boosting the precision and efficacy of DT simulations even further.

3.2 Comparison Between Cyber-Physical Systems and Digital Twins

There are two different but related ideas in the world of cutting-edge technological systems: CPS and DTs, which are interesting and important in their own ways. However, these two terms are completely different from each other. For interconnected systems that can perceive, analyze, and act upon based on the surroundings, the term CPS is used to describe the combination of computing algorithms, physical components, and communication networks. Fusion of physical elements with digital intelligence is a common component of CPS, allowing for fully or partially autonomous decision-making and control. Real-time responsiveness, adaptability, and interactivity with the physical world via sensors, actuators, and networked interfaces are the hallmarks of such systems. DTs, on the other hand, are digital representations or simulations of real-world items, operations, or infrastructure. Advanced modelling approaches and real-time data streams are used by DTs to accurately recreate their physical counterparts in terms of behavior, performance, and interdependencies. They connect the actual world with the virtual one, making it possible to track, analyze, and fine-tune all aspects of a system. DTs provide virtual hypothesis testing and validation, scenario-based performance prediction, and data-driven decision making. The primary difference between CPS and DTs is the former's intent and the latter's utility. Autonomous or partially autonomous systems that can interact with the physical world are the primary focus of CPS, which

places a premium on the integration of physical and digital elements. DTs, on the other hand, are primarily concerned with creating a digital representation and simulation of physical things for the purposes of gaining insights, optimizing performance, and providing decision-making assistance. In most cases, DTs are employed in tandem with CPS to improve the efficiency of the latter through real-time monitoring, analysis, and prediction. Despite their shared use of real-time data, sophisticated algorithms, and interconnection, the scope and application of CPS and DTs are distinct. Smart grids, autonomous vehicles, and industrial automation are just a few examples of the many CPSs that fall under the umbrella of CPS. In contrast, DTs can be adapted to specific assets, processes, or systems for in-depth examination and optimization. The difference between CPSs and DTs has been classified in Fig. 5.

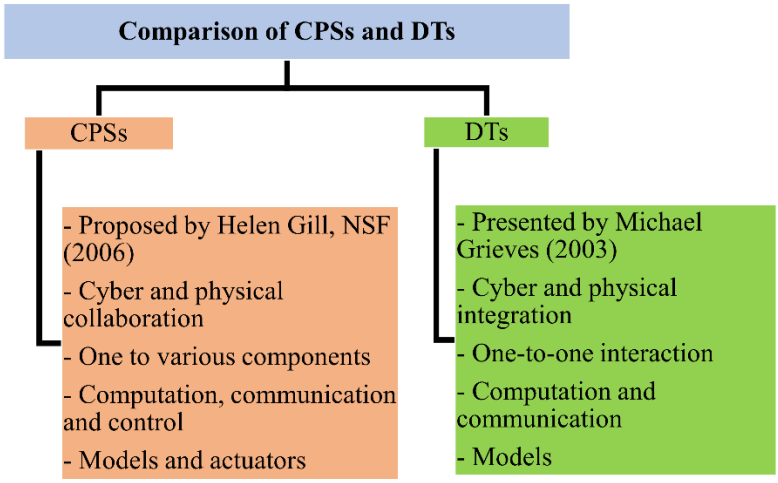

Figure 5. Difference between cyber-physical systems (CPSs) and digital twins (DTs); based on the information provided in Refs. [29,48].

3.3 Features in Cyber-physical Systems and Digital Twins

CPSs and their DT counterparts represent a physical-virtual convergence in which networked devices and sophisticated computing capabilities enable seamless integration and interaction, as shown in Fig. 6. Several important traits emerge in this context, emphasizing the distinctive nature of CPS and associated DTs. CPS and DTs have a strong link between the physical and digital components. The physical system, which consists of sensors, actuators, and real-world entities, continuously generates data, which the DT captures and processes. This interaction enables bi-directional information flow, allowing for real-time monitoring, analysis, and control of the physical system. The ability to mimic and forecast system behavior is another distinguishing property of CPS and DTs. DTs may perfectly recreate the dynamics and responses of a physical system by producing a virtual representation. These simulation capabilities can be used to estimate system performance, analyze multiple scenarios, and optimize decision-making processes, ultimately improving overall system efficiency and resilience. CPS and DTs also make advanced data analytics and AI/ML approaches possible. The massive volume of data produced by the physical system, when paired with historical data stored in DTs, enables sophisticated analysis and pattern recognition. These techniques can be used to install predictive maintenance, anomaly detection, and optimization algorithms, allowing for proactive system management and failure mitigation [49]. CPS and their DTs rely heavily on interconnectivity and interoperability. These systems are based on interconnected devices, networks, and protocols that allow for smooth communication and integration across multiple components and subsystems. Interoperability ensures compatibility and standards, simplifying information sharing and encouraging collaboration among many stakeholders such as manufacturers, operators, and service providers. Furthermore, CPS and DTs have effective cybersecurity capabilities. These systems are vulnerable to different cyber risks and attacks since they operate in a highly networked environment. To defend against unwanted access, data breaches, and system disruptions, robust security measures such as encryption, authentication, and intrusion detection systems are installed, assuring the integrity and confidentiality of important information. CPS and DTs support a scalable and adaptable design. These systems' modular design enables for

simple extension, adaption, and customization. New sensors, actuators, or capabilities can be effortlessly incorporated into existing infrastructure, ensuring scalability to meet changing needs. The flexibility of CPS and DTs allows for interoperability with other developing technologies such as cloud computing, edge computing, and the IoT, allowing for greater system integration and functionality.

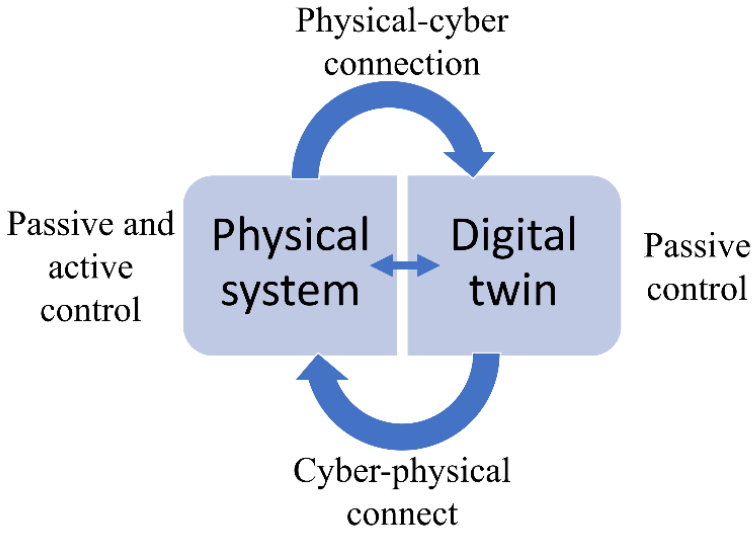

Figure 6. Cyber and physical system interaction; based on the information provided in Refs. [48,50].

3.4 Cyber-physical Systems and Digital Twins for Various Sectors

Although still in its nascent stages, CPS is catalyzing a transformative shift across diverse sectors, including manufacturing, healthcare, and transportation, by integrating control, communication, and computational capabilities. For instance, the application of CPS was explored in smart manufacturing to optimize productivity for mass production and global marketing [51]. A 5-level system architecture was proposed for implementing CPS in manufacturing, encompassing configuration, cognition, cyber, data-to-information conversion, and smart connection levels [52]. Similarly, the utilization of CPS was investigated for achieving intelligent transportation systems, focusing on traffic control, command, and information flow [53].

The role of sensors, actuators and communication networks in realizing smart traffic lights and traffic flow systems was highlighted. A comprehensive CPS architecture was presented, emphasizing computation, communication, and control, to enhance transportation services' safety and quality [54]. Nevertheless, challenges such as privacy concerns, security, testing costs, inoperability, and software/hardware access hinder the advancement of CPS [55]. These issues were addressed by designing an integrated traffic-driving-network simulator to evaluate transportation CPS efficacy. Additionally, CPS applications were explored in aviation to improve flight safety and airworthiness and in medical science for real-time risk mitigation using embedded threat detectors [56,57]. Distinct from CPS, DT primarily focuses on models and data transmission between physical artifacts and digital representations [58]. DT's application across industries remains limited compared to CPS. In manufacturing, a DT prototype was developed for optimizing adaptive behavior in production systems using automated guided vehicles [59]. The utilization of DT was explored for shop floor management systems in a logistic learning factory [60]. A conceptual framework was proposed for DT models integrating product design and manufacturing processes [61]. A DT healthcare system was provided that supervises, diagnoses, and predicts the well-being of elderly individuals [62]. A DT framework was presented for hospitals, enabling virtual health supervision, diagnostics, and future predictions based on patient data [63]. Addressing the challenges of inaccurate data specification and implementation errors is crucial for the widespread adoption of CPS [64]. Seamless and accurate information flow between the cyber and physical realms must be further improved. Recent studies have emerged to harness the capabilities of CPS and DT in various domains. A deep learning-based DT and CPS framework was developed to advance smart manufacturing [65,66]. Table 1 summarizes a few literature studies on CPS and DTs.

Table 1. Cyber-physical systems in various industries

Focusing areas	Type	References
Transport (Traffic system, service evaluation)	CPS	[53][54][55][48]
Aeronautics (Safety)	CPS	[56] [48]
Manufacturing (smartification, optimization, and management)	DT, CPS	[48,51,60]
Medical (Risk analysis, human-medicine interaction, healthcare, and hospitalization)	DT, CPS	[28,48,57,62,63]

4 Components and Role of Cyber-physical and -digital Systems

This section discusses the components of distributed digital factory (DDF), and role of localized middleware in DDF.

4.1 Components of Future Distributed Digital Factory

The components of a DDF may differ based on the specific implementation and technology used. However, below are some examples of common components:

a) These are physical machines, devices, and systems that can gather and exchange data across a digital network. Robotic arms, AM, SM sensors, and automated assembly lines are some examples.
b) IoT devices are critical components of a DDF because they collect and transmit data from numerous sources, allowing for real-time monitoring, control, and optimization. Sensors, actuators, and smart tools are examples of IoT devices.
c) For data analysis, ML/AI applications, cloud-based systems provide storage, processing capacity, and computing resources. The cloud enables centralized data administration and access from a variety of places.
d) Advanced data analytics and AI technologies are used to process the huge amounts of data generated by the DDF's many systems and equipment. To improve efficiency and productivity, AI systems can provide insights, predictive analytics, and optimization tactics.
e) To connect all components of the DDF, a strong and dependable network infrastructure is required. High-speed internet connectivity, secure communication protocols, and networking technologies such as Ethernet or Wi-Fi are all part of this.
f) A DT is a real-time virtual reproduction of a physical factory, representing its operations, systems, and assets. It enables modeling, analysis, and optimization before changes are implemented in the physical factory.
g) Collaborative robots assist human employees while increasing productivity, safety, and flexibility. Collaborative robots can do repetitive or hazardous duties, allowing human workers to focus on more complicated or creative tasks.
h) Augmented and virtual reality technologies create immersive and interactive experiences, allowing for remote training, maintenance, and troubleshooting. They can also help with quality control and inspection.
i) A DDF entails integrating suppliers, logistics, and manufacturing processes across multiple sites and organizations. Supply chain management systems, data exchange platforms, and standardized communication protocols can help with this integration.
j) In a DDF, ensuring the security of data, systems, and intellectual property is critical. To safeguard sensitive information, robust cybersecurity safeguards, encryption, access controls, and data privacy regulations are in place.

It should be noted that these components are interconnected and collaborate to form a DDF industrial ecosystem. The examples may differ depending on the implementation and industry, but they always involve the integration of physical machinery, digital technology, and data-driven decision-making processes.

4.2 Role of Local and Centralized Middleware in Distributed Digital Factory

Local and centralized middlewares are critical in facilitating DDF communication, coordination, and integration. Here's a summary of their responsibilities:

4.2.1 Local middleware

Local middleware is software and communication protocols that are implemented locally, generally within specific machines, devices, or subsystems. Its responsibilities include the following:

- It allows for the integration and communication of several machines, sensors, actuators, and other devices inside a single local area or workstation. It ensures that these devices can communicate with one another and exchange data.
- It collects and analyzes data generated in real time by local devices, sensors, and systems. It allows for local data capture, filtering, and transformation before passing it to higher-level systems for additional analysis and decision-making.
- It offers control and management capabilities for local devices. It allows you to monitor, configure, and coordinate operations within a given machine or subsystem.
- It enables real-time communication and interaction between devices, allowing them to collaborate, synchronize, and coordinate their operations within their immediate surroundings.
- Local faults or anomalies, such as device failures or communication issues, can be detected and handled. It may include fault tolerance, error recovery, and local system resilience techniques.

4.2.2 Centralized middleware

In the DDF design, centralized middleware runs at a higher level. It is concerned with controlling and organizing interactions among various local locations, workstations, or subsystems. Its responsibilities include the following:

- It combines information gathered from numerous local regions and devices. It combines, fuses, and aggregates data to create a comprehensive view of the factory's operations, procedures, and performance.
- It controls and orchestrates workflows across several local areas, coordinating tasks, activities, and process execution. It ensures correct operation sequencing, synchronization, and optimization across production.
- It optimizes the distribution of resources across the DDF, such as equipment, supplies, and employees. It considers aspects such as workload balance, priority-based scheduling, and optimal resource use.
- It allows for the integration and communication of many domains or subsystems within the factory, such as production, logistics, quality control, and maintenance. It enables data sharing, coordination, and cooperation across domains.
- It facilitates decision-making by providing advanced analytics, predictive modeling, and optimization algorithms. It uses aggregated data from several localities to develop insights, identify patterns, and enable data-driven decision-making.
- It ensures the DDF's security, privacy, and access control measures. To safeguard sensitive data and prevent unwanted access, it manages authentication, authorization, and encryption.

5 Security Considerations and Mitigations in Distributed Digital Factory

In the last decade, frequent cyber-attacks have been observed in the manufacturing industry. The aim behind these attacks is to disrupt the manufacturing plants to affect the community and the overall country's finances. In most cases, these attacks are generated from outside the country, or actors are handled across the border. As per the Microsoft defense digital report published in 2021 [67], nation-state attacks mostly originated from Russia 58%, North Korea 23%, Iran 11%, and China 8%. Nation-state attacks are defined as cyber-attacks carried out by a government against another state, or organization. These attacks involve highly sophisticated techniques and use significant resources to target critical infrastructure. The main aim is financially hit other states, gain illegal access to the information, and disrupt operations. In 2017, cyber-attacks were reported on manufacturing industries including Renault, Saint-Gobain, Rosnef, and Merck [68]. Renault's entire production was shut down for the complete day cost several million dollars. The cyber-attacks on manufacturing sites not only compromise the production cycle deadline but also add up to the customers confidentiality. Table 2 highlights significant attack events that have inflicted considerable damage on the global industry. These incidents have sparked a heightened interest in cyber-attacks targeting Cyber-Physical Systems.

Table 2**.** Cyber-attacks on industries; reproduced from Ref. [69].

Country	**Details**
Iran (2010)	Stuxnet attack - destroying controller
Ukraine (2015)	Black energy attack on power grid
Russia, India, China (2017)	Ransomware attack – WannaCry
Czech Republic (2020)	Cyber-attack on hospital
US Health Service (2020)	Cyber-attack on health system servers
US Colonial Pipeline (2021)	Ransomware attack on fuel pipeline

5.1 Adversarial Attacks over Machine Intelligence

With the inception of Industry 5.0, the digital factory relies on machine intelligence to optimize its production and learn from historical data. However, machine learning models are vulnerable to various attacks that can be injected through digital connectivity with the system. These attacks can be launched through inside resources or sometimes, the system vulnerabilities are used to inject malware into the system. In this section, we have highlighted the potential attacks on machine intelligence. A typical machine learning system follows a generalized data processing pipeline that starts with data input from distributed sensors placed to monitor the manufacturing machines. The gathered data is transferred into a digital domain where it is cleaned before applying the machine learning model. Finally, the decision is based on the machine learning output. During this pipeline process, an adversary can attempt to manipulate the data collection process or data processing to corrupt the target model and temper the original output. The main attacks are summarized below [70]:

- Evasion Attack - in this attack the adversary manipulates the input data to deceive the model and cause it to make incorrect predictions. The main aim of such attacks is to exploit vulnerabilities in the learning model, allowing attacker to bypass the classification mechanism.
- Poisoning Attack, the adversary contaminates the training data during the model training time. With significant knowledge of the machine learning model, an adversary tries to inject the samples to compromise the learning process.
- Exploratory Attack, the learning models are treated as a black box where internal workings are not easily interpretable; therefore, an adversary submit designated inputs to observe the model response and use this information for inference about structure, training methodology and weaknesses.

In digital twin systems that are based on machine learning models deployed online for inference. It is important to protect the model confidentiality especially if the fraud or anomaly detection is based on the ML models, knowing the model means adversaries can evade the detection process. In model extraction, the adversary constructs its model that mimics the original model [4]. In this way, the adversary duplicates the functionality of the original. During the reconnaissance phase, the digital twin is accessed as a black box, therefore, only results are available to the adversary. However, sometimes the model provides rich content such as confidence value and class labels. The adversary can exploit this information to perform the model extraction attack. The key processes of model extraction attacks include query input design, confidence values collection, and attack with equation-solving and patch-finding.

5.2 Adversarial Attacks over Connected Manufacturing System

The sensors play a crucial role in the functioning of DDF. The DDF integrates the capabilities of sensing, computation, and actuation by networking different devices together. These systems heavily rely on sensors to gather real-world data, process it through connected processors, and control actuators accordingly. Bridging the physical and cyber realms, DDF enables seamless communication and coordination between sensors, processors, and actuators, facilitating efficient and effective operation in diverse applications. DDF is an integration of communication and control within physical systems. The inclusion of a communication network is crucial for enhancing the effectiveness of distributed manufacturing machines. However, this simultaneously exposes the

control system to various security and privacy threats, albeit unintentionally. The rise of the Internet of Things (IoT), Cyber-Physical Systems (CPSs), and other rapidly advancing techniques that heavily depend on precise sensor data has brought attention to the escalating concern of cyber-attacks. The affordability and energy-efficient nature of sensors make them vulnerable to hacking, thus posing a significant security challenge. Additionally, DDF heavily rely on network-based data communication, making them susceptible to various types of attacks.

5.2.1 Potential Attacks

Fig. 7 depicts a typical machine connection within the context of a DDF, showcasing the integration of various sensors to digitize manufacturing processes. In the AM domain, sensors such as pyrometers, pressure sensors, infrared cameras, high-speed imaging cameras, acoustic sensors, and collision avoidance sensors are deployed. These sensors enable temperature monitoring, gas pressure measurement, thermal anomaly detection, capturing fast-moving processes, monitoring vibrations and sounds, and ensuring safe navigation by detecting obstacles. Similarly, in the subtractive manufacturing (SM) domain, sensors such as position and displacement sensors, force sensors, tool wear sensors, and temperature sensors are employed. These sensors facilitate precise positioning of tools and workpieces, measurement of cutting forces and tool wear, monitoring of tool condition and performance, and environmental temperature monitoring. In the case of robotic arms, sensors like position and orientation sensors, force/torque sensors, proximity sensors, vision sensors, and tactile sensors are utilized. These sensors enable accurate tracking of the arm's position and orientation, measurement of forces and torques during manipulation tasks, detection of object presence or proximity, visual perception and object recognition, and feedback on contact and surface properties. The real-time data provided by these sensors plays a crucial role in maintaining optimal conditions, detecting abnormalities, and ensuring quality throughout the manufacturing process within a DDF.

There are multiple stages where attacks can be launched on sensors within DDF. Firstly, at the sensor reception stage, attackers can manipulate the information that the sensor receives from its environment - influencing the monitored environmental conditions, and adversaries can manipulate the data gathered by the sensor. Secondly, in the perception stage, attacks exploit design oversights to gain control over the system. These attacks specifically target the control algorithms, including machine learning algorithms, that are responsible for processing and interpreting the received sensor data. Through disrupting the decision-making process, adversaries can manipulate the system's behavior and outcomes. Lastly, communication stage attacks focus on compromising the communication between the sensor and the rest of the system – exploiting vulnerabilities in the communication protocols or network infrastructure, attackers can intercept, modify, or disrupt the transmission of sensor data, potentially leading to incorrect or misleading information being processed by the DDF. These attack stages highlight the importance of robust security measures to safeguard sensors and the communication channels within factory environment, as they are critical components for accurate data acquisition and reliable decision-making processes. However, it is essential to acknowledge the potential attacks that can target DDF, as depicted in Fig. 7.

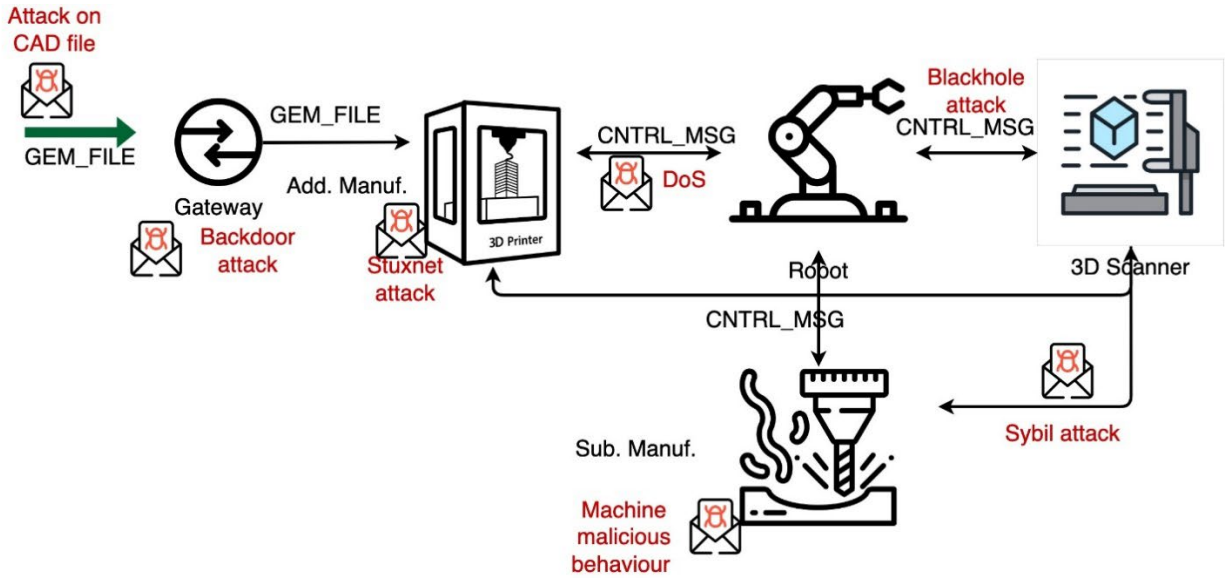

Figure 7. Distributed digital factory – Machine connectivity and attack mapping.

The attacks, including Denial of Service (DoS), Blackhole, Sybil, Backdoor, poisoning, exploration, and evasion attacks are explained in Table 3.

Table 3**.** Cyber-attacks on Industries; reproduced from Ref. [71,72].

Attacks	Details
Denial-of-service (DoS)	Denial of Service (DoS) attack on a Cyber-Physical System (CPS) manufacturing system aims to disrupt or impair the system's normal operation by overwhelming its resources or causing system malfunctions – it involves flooding the system with an excessive number of requests or data, effectively exhausting the system's processing capabilities or network bandwidth.
Blackdoor	Backdoor attack involves the unauthorized insertion of hidden access points or vulnerabilities into the system's software or hardware. These backdoors allow attackers to gain illicit access to the system, bypassing normal authentication and security measures.
Stuxnet	The Stuxnet attack is highly sophisticated and unprecedented cyber-attack specifically targeting a Cyber-Physical System (CPS) involved in manufacturing. It was designed to exploit vulnerabilities in industrial control systems, allowing it to spread through networks and specifically target programmable logic controllers (PLCs).
Blackhole	Blackhole attack refers to a malicious activity where a compromised or malicious device or node within the system selectively drops or intercepts incoming data packets or messages, rendering them inaccessible. The attacker strategically manipulates the routing or forwarding behavior to divert traffic to the compromised node, which then discards the received data without forwarding it to its intended destination.
Sybil	It is a type of malicious activity in which an adversary creates multiple fake identities or nodes within a network to deceive and manipulate the system. It involves an attacker creating multiple counterfeit entities that masquerade as legitimate nodes in the network.
Data Poisoning	Data Poisoning attack is a type of malicious activity where an adversary intentionally manipulates or contaminates the data used for training or decision-making processes.

5.2.2 Attack Defenses

In cases where the malicious actor possesses a certain level of control over the sensing environment or can significantly influence it, they can manipulate the data acquired by a targeted sensor. Exploiting these vulnerabilities, they can aim to compromise the entire system by generating misleading information that triggers incorrect responses or gradually introduces errors over time, leading to significant consequences known as a meaningful response. Petit et al. [28] discuss common countermeasures against such attacks based on sensor redundancy and random sampling techniques. Sensor redundancy, also known as sensor fusion, is a defensive

strategy that involves using multiple sensors of the same type, make, and model to sample the environment. This redundancy enhances system performance by increasing the accuracy of environmental understanding and mitigating the effects of noise. However, when sensors provide significantly divergent readings, the system can identify and respond to malicious activity [73]. Random sampling is another useful defensive technique where the timing of sensor sampling is determined randomly [28]. This approach can be effective in countering attacks that rely on predicting the timing of sensor responses, such as lidar spoofing; however, this technique becomes ineffective against continuous attacks. In situations where the timing of sensor sampling is not crucial, random sampling may not provide significant protection. Metzen et al. [74] proposed the creation of a subnetwork capable of identifying artificially perturbed data. This information can be utilized by a system evaluating sensor data to disregard inputs categorized as artificial.

6 Open Standards for Distributed Digital Factory

The DDF systems will be designed to promote openness, which refers to the ability to integrate and collaborate with various stakeholders, technologies, and data sources. Openness enables seamless communication and interoperability between different components, machines, software, and systems involved in digital manufacturing. It allows for data sharing, exchange, and collaboration, leading to enhanced efficiency, innovation, and productivity in the manufacturing ecosystem. These systems usually develop with scalability in mind, allowing for the flexible and efficient expansion of digital manufacturing capabilities. Scalability ensures that the systems can adapt and accommodate increasing demands, whether it's scaling up the production capacity, integrating new machines or technologies, or handling larger volumes of data. By being scalable, the systems can meet the evolving needs of the manufacturing industry, supporting growth and adaptability in a dynamic market environment.

Pei et al. [75] focused on the need for efficient data transfer standards in the context of decentralized cloud manufacturing. The existing data exchange standards, such as STL, have limitations in supporting the re-manufacturing landscape. The authors evaluated alternative standards like AMF, 3MF, STEP, and STEPNC, highlighting their features, advantages, and contributions. Interviews and surveys with experts in AM and RDM provide insights into the most important data transfer features. The STL file format, commonly used for transferring data models in additive manufacturing (AM), has limitations such as redundant information, geometrical defects, and the inability to store material, texture, and structural information [6]. These shortcomings make it less suitable for advanced AM machines. The AMF and the 3MF format are two notable efforts in the field of additive manufacturing. AMF is an official ISO/ASTM standard for AM, while 3MF was developed to enhance compatibility between hardware and software systems. Both formats utilize the extensible markup language (XML) as a standardized, text-based, human-readable encoding format, following the open XML specification [76]. In addition to the aforementioned standards, there are several other notable standards that are widely used in the manufacturing industry to facilitate various aspects of operations. These standards play a crucial role in ensuring interoperability, data exchange, and communication across different systems and organizations.

6.1 Open Platform Communications Unified Architecture

Open Platform Communications Unified Architecture (OPC UA) is an open standard that facilitates information exchange in industrial communication, enabling seamless communication among devices within machines, between machines, and from machines to systems [77]. It is recognized as the recommended industrial communication standard in the Reference Architecture Model Industry 4.0 (RAMI 4.0). OPC UA offers a comprehensive solution by providing both a communication protocol and an information modeling method, simplifying the modeling and development of digital twins for manufacturing equipment in the digital realm.

6.2 ECMA-363

ECMA-363 is a data exchange standard specifically designed for manufacturing systems [78]. It provides a common framework and guidelines for exchanging data between various components and subsystems within a manufacturing environment. The standard defines a set of rules and structures for representing manufacturing-related information, such as product models, process data, and production schedules. With ECMA-363, manufacturing systems can achieve seamless interoperability and integration between different software applications, equipment, and devices involved in the production process. The standard ensures that data is

formatted and communicated in a consistent and standardized manner, enabling efficient data exchange and collaboration among different entities within the manufacturing system.

6.3 Initial Graphics Exchange Specification

Initial Graphics Exchange Specification (IGES) is a standardized data format utilized in computer-aided design (CAD) systems to exchange 3D geometry data [79]. Its purpose is to enable interoperability between various CAD software applications and platforms. IGES establishes guidelines and data structures for representing geometric models, encompassing solids, surfaces, and wireframes, along with attributes such as color and material properties. By supporting smooth data exchange between CAD systems operating on diverse hardware and software environments, IGES plays a crucial role. Despite its limitations compared to newer formats like STEP, IGES remains widely utilized as a legacy format for sharing CAD data across different systems.

6.4 Requirements Interchange Format

Requirements Interchange Format (ReqIF) is a standardized format for exchanging requirements in systems engineering using system modeling language [80]. It allows structured representation, storage, and sharing of requirements across diverse tools and platforms. ReqIF ensures consistency and traceability of requirements throughout the systems engineering lifecycle, promoting collaboration and integration. It acts as a bridge between system modeling tools, enabling seamless transfer of requirements while maintaining their structure and context.

6.5 ISO-14306:2017

ISO-14306:2017 is a standard that facilitates the exchange of high-quality product data [81]. It establishes a structured format for sharing accurate and consistent product information between organizations and systems. By following this standard, organizations can ensure smooth communication, interoperability, and data integrity across the entire product lifecycle. The standard provides guidance on organizing data, including metadata, validation rules, and quality metrics, which enables efficient and reliable exchange of product data. Ultimately, ISO 14306:2017 fosters effective collaboration and integration among various stakeholders engaged in product development and management.

6.6 National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is actively involved in various initiatives to address the needs of Smart Manufacturing Systems (SMS). These initiatives include; developing a reference architecture for Cyber-Physical Systems (CPS) at NIST [82]; creating new standards for Digital Thread and Model-Based Engineering [83]; Establishing a reference architecture and standards for leveraging big data in SMS [84]; collaborating with OAGi to develop standards for cloud-based services in manufacturing; Leading an effort on cyber security for industrial systems, which is of significant importance to manufacturers [85]; coordinating the deployment of advanced manufacturing institutes across the United States; These institutes specialize in various areas of advanced and smart manufacturing and aim to transfer research capabilities into practical production. Through these initiatives, NIST is actively working towards advancing and promoting smart manufacturing by developing frameworks, standards, and collaborative efforts that enable the seamless integration of cutting-edge technologies and research into industrial production processes.

7 Development of Digital Twin

This section discusses digital twin (DT) and state-of-the-art in DT.

7.1 Definition of Digital Twin

A DT is a virtual replica of a functioning object or physical process. Its purpose is to accurately represent the object or process in a virtual environment. This is achieved using multiple sensors that capture data from the physical system and feed it to the digital twin. According to NASA's Modeling, Simulation, Information Technology & Processing Roadmap 2010, a DT is described as an integrated multi-physics, multi-scale, probabilistic simulation of a vehicle or system that utilizes the best available physical models, sensor updates, and fleet history, to mirror the life of its real-world counterpart [86]. Therefore, DT simulates the physical process while incorporating real-time monitoring and control of the physical counterpart. A DT is a virtual replica of a functioning object or physical process. Its purpose is to accurately represent the object or process in a virtual environment. This is achieved using multiple sensors that capture data from the physical system and feed it to the digital twin. According to NASA's Modeling, Simulation, Information Technology & Processing Roadmap 2010, a DT is described as an integrated multi-physics, multi-scale, probabilistic simulation of a vehicle or system that

utilizes the best available physical models, sensor updates, and fleet history, to mirror the life of its real-world counterpart [86]. Therefore, DT simulates the physical process while incorporating real-time monitoring and control of the physical counterpart.

DTs can be used to predict, monitor, optimize or study the concerned physical phenomenon virtually [87]. A DT combined with real-time control and two-way interaction between the object or process and the virtual replica results in a cyber-physical system. Time period of "real-time interactions" is often subjective and can vary from a few microseconds to few hours depending on the physical phenomenon. With advancements in controls, monitoring, artificial intelligence and machine learning, definition of a DT is being evolved rapidly. Different terms such as digital environments, digital prototypes, digital models, digital shadows are used with varying levels of complexity for the developed replica [88], as shown in Fig. 8.

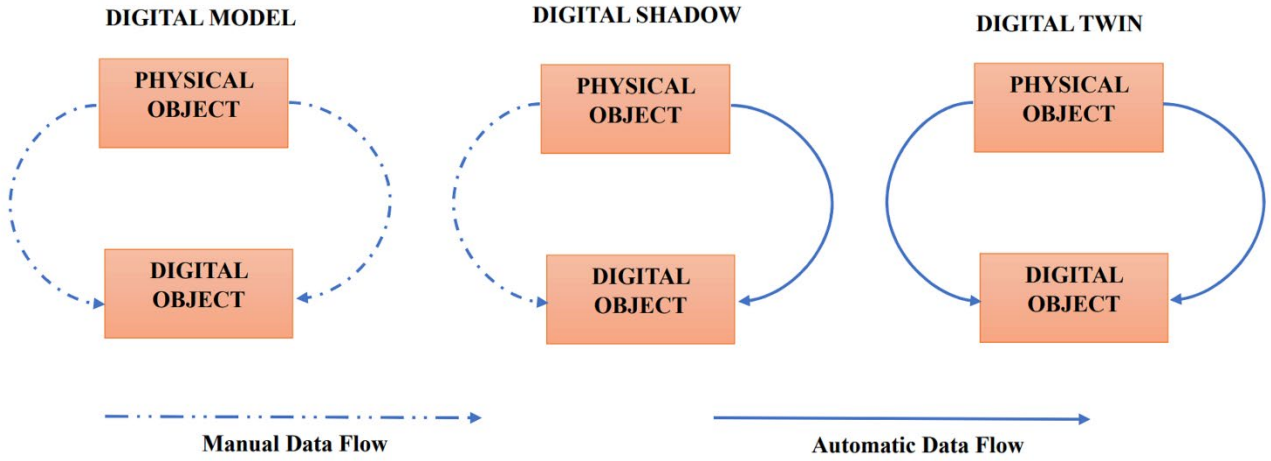

Figure 8. Variation of complexity in physical-digital object integration in different levels; based on the information in Ref. [88].

7.2 Current State-of-the-art

The development of DTs began even before the term was coined by Michael Grieves in 2003 during his research on product lifecycle management [89]. Various industrial leaders such as Rolls Royce, General Electric, and Siemens have been using simulations for the design and analysis of mechanical components in product development. However, the development of a simulation model into a DT requires certain requirements. A DT is dynamic in nature as it continuously monitors the functioning of the physical entity, predicts possible outcomes or properties of concern, and controls significant influencing parameters to achieve desirable characteristics. This is accomplished through bidirectional data transfer between the physical and digital counterparts. One significant criterion that a digital model or digital shadow fails to address is the incorporation of artificial intelligence. A comprehensive DT model should be capable of learning from both real and simulated data about its environment to make decisions that help achieve the desired characteristics, thereby imparting a form of autonomy to the model.

Various researchers have recently developed different levels of DTs for AM and SM systems. These systems can be categorized into different levels within a digital twin hierarchy based on factors such as autonomy, data transfer, monitoring, and real-time control. Phua et al. [90] introduced a DT hierarchy specifically for metal additive manufacturing. This hierarchy consists of four verticals: implicit, instantiated, interfaced, and intelligent DTs. Fig. 9 provides a schematic representation of this hierarchy.

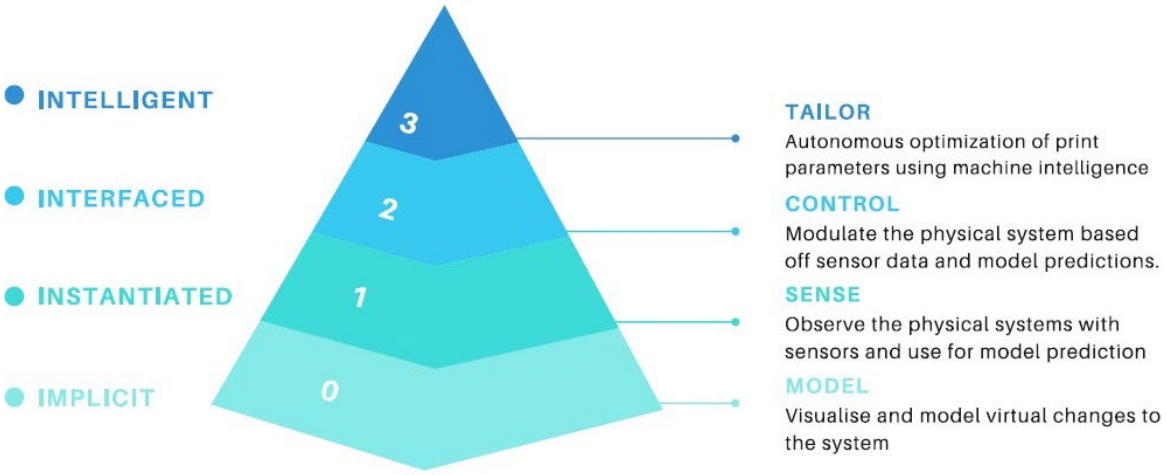

Figure 99. Hierarchy of a metal AM digital twin [90]; with permission from publisher.

7.3 Preliminary Work in Using Digital Twin for Creating Distributed Digital Factory

The concept of cyber-physical systems (CPS) was systematically defined in 2015. Lee et al. [52] proposed the connection of components' cyber-twin, which can provide self-awareness and self-prediction, to achieve CPS, as depicted in Fig. 10.

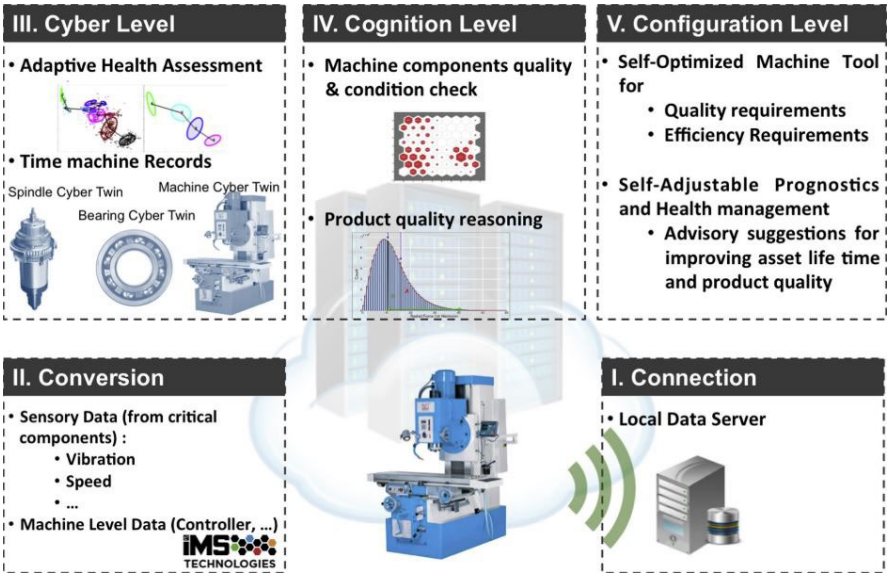

Figure 1010. Cyber-twin components and workflow [52]; with permission from publisher.

Subsequently, Vijayakumar et al. [91] integrated DTs with distributed manufacturing to establish a distributed digital factory. The research involved developing a digital assembly line capable of monitoring machine status, workpiece location, and identifying defective parts, as depicted in Fig. 11. This schematic provides an illustrative representation of the digital factory.

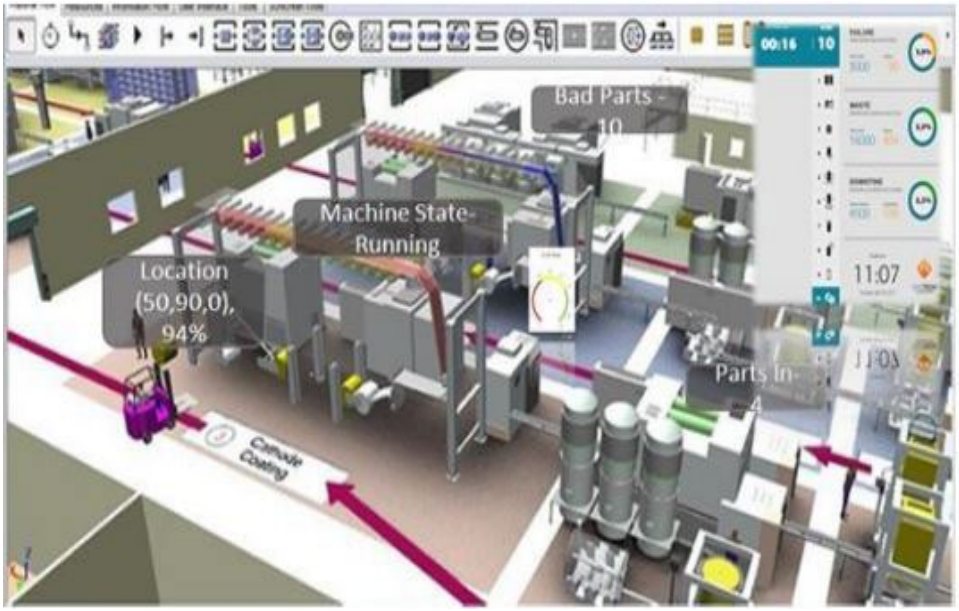

Figure 1111. Digital factory architecture [91]; published under open-access license.

To expand the application of DTs in the creation of a DDF, Park et al. [92] devised and executed a DT for a micro smart factory. In this instance, the DT encompassed not only machine models but also DTs for robotic arms and CNC machines, as illustrated in Fig. 12. Given the self-prediction and self-awareness capabilities of DTs, data collection is commonly employed in the design of digital factories.

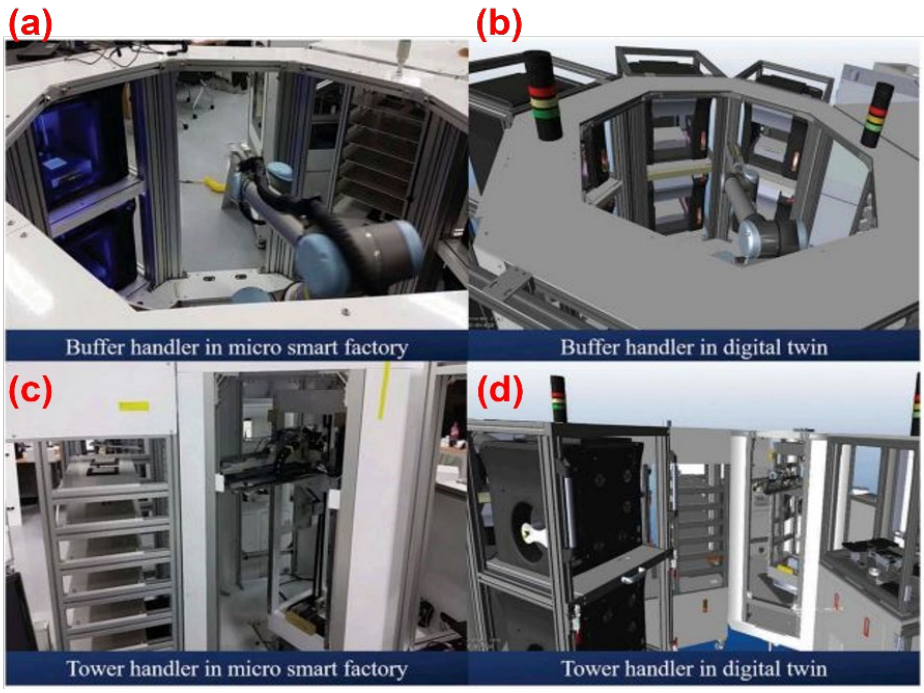

Figure 1212. Synchronization of digital smart factory **(a)** physical buffer handler by robotic arm, **(b)** digital twin of buffer handler by robotic arm, **(c)** physical CNC tool tower handler, and **(d)** digital twin of CNC tool tower handler [92]; with permission from publisher.

Liu et al. [93] organized the structure of data that could be collected during the development of a digital factory, as depicted in Fig. 13. The digital factory incorporated the potential process parameters of AM. While numerous ML/AI techniques have been applied in manufacturing, there still exists a gap between the development

of digital factories and the effective utilization of ML/AI in the development process, which warrants further exploration.

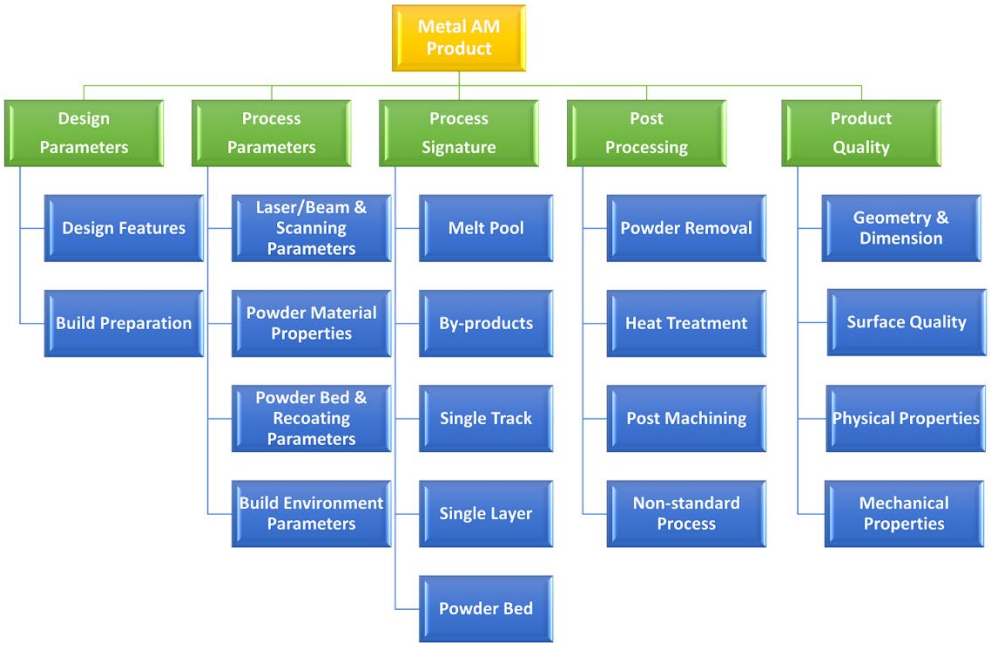

Figure 1313. Structure of metal AM data model; based on the information in Ref. [93].

7.4 Tools for Digital Twin Development: Research, open-source, and Commercialized software

The development of a DT is a complex process that necessitates knowledge and expertise across multiple domains. Qinlin et al. [46] conducted a comprehensive review of enabling technologies and tools for DT development. The various tools for DT development were categorized broadly as follows: tools for the physical world, tools for DT data, tools for DT services, tools for DT modeling, and tools for connections in DT. Each category comprised several sub-categories, as illustrated in figure 14.

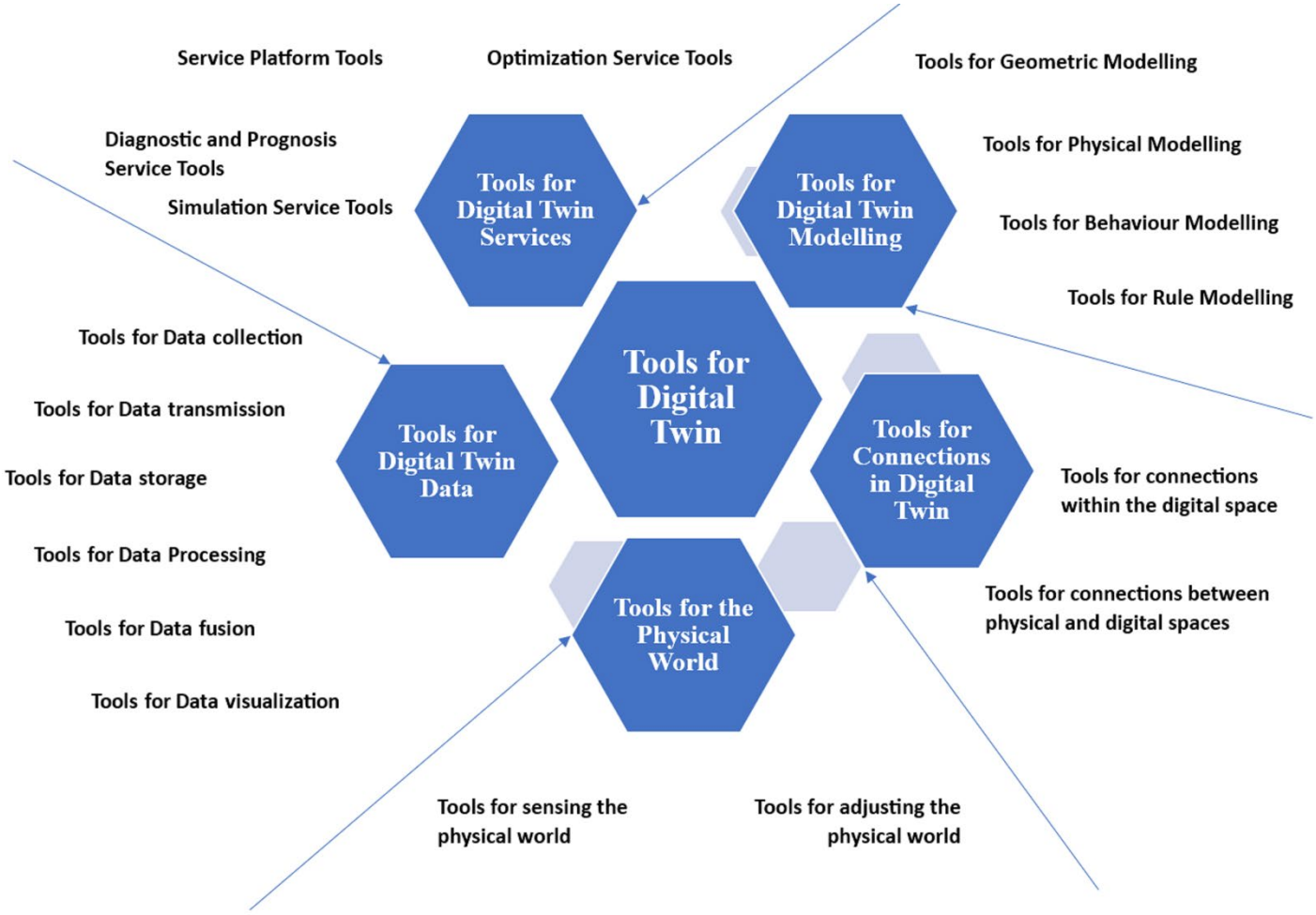

Figure 1414. Framework of tools for digital twin; based on the information in Ref. [46].

Currently, an increasing number of companies and researchers are actively engaged in the development of tools for DTs. This has resulted in the availability of several comprehensive open-source, commercial, and research software and tools that facilitate DT development. Table 4 provides a comparison of the capabilities of leading software and tools for DTs [46]. Sergey et al. [94] established an evaluation criterion and compared the tools for developing DTs throughout the lifecycle of manufacturing systems. Most of the available tools' focus on multiple capabilities rather than being limited to a single dimension. For instance, ANSYS Twin Builder offers capabilities such as geometric modeling, finite element analysis, data analysis, optimization, and troubleshooting. Currently, an efficient DT development process requires the combination of various enabling tools. However, the lack of a common format and protocols among these tools poses a hindrance to their simultaneous use, which needs to be addressed to ensure the efficient utilization of these available tools for DT development.

Table 44. Comprehensive Tools and their roles in different aspects of digital twin [46]; with permission from publisher.

		Predix	PTC Thingworx	Siemens Mindsphere	ANSYS	Dassault 3D Experience	Foxconn's Beacon
DT Evolution	Knowing the physical world	-	-	-	✓	✓	-
	Changing the physical world	✓	-	✓	-	-	-
Modelling	Geometry modelling	-	-	-	-	✓	-

	Physical modelling	-	-	-	✓	✓	-
	Behavior modelling	-	-	-	✓	-	-
	Rule modelling	-	✓	-	-	-	-
DT Data Management	Data Collection	✓	✓	✓	-	-	✓
	Data Transmission	-	✓	✓	-	-	-
	Data Storage	-	✓	-	-	✓	✓
	Data processing	✓	-	-	-	✓	✓
	Data Fusion	✓	-	-	-	✓	✓
	Data Visualization	-	-	-	-	✓	✓
Services	Simulation services	✓	-	✓	✓	✓	✓
	Optimization services	✓	-	✓	-	-	✓
	Diagnosis and Prognosis services	✓	✓	✓	✓	-	✓
	Platform Services	✓	✓	✓	-	✓	✓
Connections	Connection in Digital world	✓	-	✓	-	✓	✓
	Connection between digital and physical world	✓	✓	✓	-	✓	✓

7.5 Datasets available for Digital Twin Training

The development of DTs is rapidly progressing to incorporate real-time control of their physical counterparts. This involves the utilization of machine learning methods to predict probable outcomes based on real-time monitored parameter values, followed by adjusting the corresponding parameters as suggested by the ML model. This infusion of autonomy into the DT enables it to achieve the highest level of the DT hierarchy - interfaced and intelligent DTs. However, the accuracy of ML predictions relies on the availability of pertinent high-fidelity data to train the model. The presence of extensive high-fidelity datasets improves the process mapping during the training of the ML model, resulting in enhanced accuracy for optimization during DT operation. Consequently, the availability of relevant high-fidelity datasets holds significant importance in the development of DTs.

The manufacturing sector stands to gain significant benefits from recent advancements in AI, data science, and ML. These advancements can contribute to improvements in manufacturing quality, waste reduction, quality checks, and process cost optimization. Currently, there are multiple sources of data available. The progress in global network connectivity over the past decade has enhanced data accessibility through various repositories and open-source websites. Table 5 provides a list of websites that offer data on manufacturing and technology-related topics, which can be valuable for DT development.

Table 55. List of few datasets available for digital twin development.

Source	Domain
Kaggle Datasets	https://www.kaggle.com/datasets
Google Datasets	https://datasetsearch.research.google.com/
U.S. Government's Open Data	https://data.gov/
National Institute of Standards and Technology	https://www.nist.gov/el/ammt-temps/datasets
Fraunhofer Big Data AI	https://www.bigdata-ai.fraunhofer.de/s/datasets/index.html
Data world	https://data.world/

8 Research Gaps and Future Directions

Based on the results, the following research gaps and future directions can be identified:

- Existing digital factory research has concentrated on digital twins (DTs), additive manufacturing (AM), subtractive manufacturing (SM), and some security issues. However, a comprehensive approach that includes the integration of devices with dynamic provisions to activate DTs via the distributed digital factory (DDF) idea is required. Future studies should investigate and create frameworks that allow for the seamless integration and interaction of physical and digital systems in DDFs.
- Further research into the components of cyber systems utilized in DDFs is required. This entails a thorough examination of AM and SM equipment, sensors, communication protocols, and monitoring software. The focus of research should be on establishing efficient and optimal cyber-physical systems that allow for effective coordination and synchronization of physical and digital elements in DDFs.
- The issues associated with the design and deployment of DDFs should be addressed through research, with a focus on security, scalability, and interoperability. This includes adopting strong security measures to safeguard the integrity and confidentiality of DDF data and systems. Furthermore, scalable frameworks should be investigated to handle the different locations and capabilities of DDF vendors and participants. To enable seamless communication and collaboration among different components and systems inside DDFs, interoperability standards and protocols should be defined.
- Future research should focus on the creation of open frameworks for DDFs, which will allow system integration from vendors and participants with various locations and skills. Within the DDF ecosystem, this would promote collaboration, knowledge sharing, and resource optimization.
- The development and deployment of scalable and safe frameworks should be prioritized in DDF implementation. This ensures the dependability and availability of the DDFs' on-demand manufacturing operations. The focus of research should be on building and implementing frameworks that can support variable production requirements while effectively addressing security concerns.

Addressing these research gaps and focusing on the indicated future initiatives would allow the field of DDFs to progress toward more efficient, secure, and networked manufacturing systems.

9 Conclusions

This study sheds light on the current state of research in digital factories (DF) and distributed digital factories (DDFs). The concept of a DF has evolved as a powerful integration of physical and digital systems, leveraging the capabilities of additive and subtractive manufacturing (AM and SM) to enable decentralized component production. The concept of distributed digital factory (DDF) is novel and requires significant attention from research community. This research sought to fill that void by giving a thorough examination of the cyber-physical and digital systems utilized within DDFs. The components of cyber systems, especially AM and SM equipment, sensors, communication protocols, and monitoring software, have been intensively investigated. Furthermore, the difficulties in designing and deploying DDFs, such as security, scalability, and interoperability, have been highlighted. One significant finding of this study is the importance of an open framework for DDF development. This type of architecture enables smooth system integration by allowing vendors and stakeholders from various

locations and capacities to participate. This emphasis on openness fosters collaboration, knowledge exchange, and resource optimization within the DDF ecosystem. Furthermore, the study emphasizes the crucial need of a scalable and secure framework for DDF implementation success. Such a framework contributes to the overall reliability and efficiency of DDF operations by ensuring the dependability and availability of on-demand manufacturing processes.

Acknowledgement

The support provided by Intelligent Systems Center (ISC) is appreciated. This work was partially supported by the Missouri University of Science and Technology's Kummer Institute for Student Success, Research and Economic Development through the Kummer Innovation and Entrepreneurship Doctoral Fellowship.

References

[1] Tyagi AK, Fernandez TF, Mishra S, Kumari S. Intelligent Automation Systems at the Core of Industry 4.0 2021:1–18. https://doi.org/10.1007/978-3-030-71187-0_1.

[2] Kühn W. Digital factory - Simulation enhancing the product and production engineering process. Proc - Winter Simul Conf 2006:1899–906. https://doi.org/10.1109/WSC.2006.322972.

[3] Zhong RY, Xu X, Klotz E, Newman ST. Intelligent Manufacturing in the Context of Industry 4.0: A Review. Engineering 2017;3:616–30. https://doi.org/10.1016/J.ENG.2017.05.015.

[4] Kumar S, Gopi · T, Harikeerthana · N, Munish ·, Gupta K, Gaur V, et al. Machine learning techniques in additive manufacturing: a state of the art review on design, processes and production control. J Intell Manuf 2022 341 2022;34:21–55. https://doi.org/10.1007/S10845-022-02029-5.

[5] Chandra Sekaran S, Yap HJ, Musa SN, Liew KE, Tan CH, Aman A. The implementation of virtual reality in digital factory—a comprehensive review. Int J Adv Manuf Technol 2021;115:1349–66. https://doi.org/10.1007/s00170-021-07240-x.

[6] What is a Digital Factory? | TIBCO Software n.d.

[7] Liu M, Fang S, Dong H, Xu C. Review of digital twin about concepts, technologies, and industrial applications. J Manuf Syst 2021;58:346–61. https://doi.org/10.1016/J.JMSY.2020.06.017.

[8] Wu X, Zhu X, Wu GQ, Ding W. Data mining with big data. IEEE Trans Knowl Data Eng 2014;26:97–107. https://doi.org/10.1109/TKDE.2013.109.

[9] Mehdi N, Starly B. A Simulator Testbed for MT-Connect Based Machines in a Scalable and Federated Multi-Enterprise Environment. Proc - Winter Simul Conf 2019;2019-Decem:2178–89. https://doi.org/10.1109/WSC40007.2019.9004928.

[10] Herstatt C, von Hippel E. From experience: Developing new product concepts via the lead user method: A case study in a "low-tech" field. J Prod Innov Manag 1992;9:213–21. https://doi.org/10.1016/0737-6782(92)90031-7.

[11] Mcharek M, Hammadi M, Azib T, Larouci C, Choley JY. Collaborative design process and product knowledge methodology for mechatronic systems. Comput Ind 2019;105:213–28. https://doi.org/10.1016/J.COMPIND.2018.12.008.

[12] Ming XG, Yan JQ, Lu WF, Ma DZ. Technology Solutions for Collaborative Product Lifecycle Management-Status Review and Future Trend n.d. https://doi.org/10.1177/1063293X05060135.

[13] Rawat P, Singh KD, Chaouchi H, Bonnin JM. Wireless sensor networks: A survey on recent developments and potential synergies. J Supercomput 2014;68:1–48. https://doi.org/10.1007/s11227-013-1021-9.

[14] Duray R, Ward PT, Milligan GW, Berry WL. Approaches to mass customization: configurations and empirical validation. J Oper Manag 2000;18:605–25. https://doi.org/10.1016/S0272-6963(00)00043-7.

[15] Nambisan S. Designing Virtual Customer Environments for New Product Development: Toward a Theory. Https://DoiOrg/105465/Amr20027389914 2002;27:392–413. https://doi.org/10.5465/AMR.2002.7389914.

[16] Target Provides Update on Data Breach and Financial Performance n.d.

[17] After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix | WIRED n.d.

[18] Turk RJ. Cyber Incidents Involving Control Systems 2005. https://doi.org/10.2172/911775.

[19] Urbina DI, Giraldo J, Cardenas AA, Tippenhauer NO, Valente J, Faisal M, et al. Limiting the impact of stealthy attacks on Industrial Control Systems. Proc ACM Conf Comput Commun Secur 2016;24-28-

Octo:1092–105. https://doi.org/10.1145/2976749.2978388.
[20] Operation Aurora | CFR Interactives n.d.
[21] Bilge L, Dumitras T. Before we knew it: An empirical study of zero-day attacks in the real world. Proc ACM Conf Comput Commun Secur 2012:833–44. https://doi.org/10.1145/2382196.2382284.
[22] Song TW, Yang CS. A connectivity improving mechanism for ZigBee Wireless Sensor Networks. Proc 5th Int Conf Embed Ubiquitous Comput EUC 2008 2008;2:495–500. https://doi.org/10.1109/EUC.2008.71.
[23] Gandomi AH, Chen F, Abualigah L. Machine Learning Technologies for Big Data Analytics. Electron 2022;11:2–5. https://doi.org/10.3390/electronics11030421.
[24] Grossman RL. The case for cloud computing. IT Prof 2009;11:23–7. https://doi.org/10.1109/MITP.2009.40.
[25] Iwata K, Onosato M, Teramoto K, Osaki S. A Modelling and Simulation Architecture for Virtual Manufacturing Systems. CIRP Ann 1995;44:399–402. https://doi.org/10.1016/S0007-8506(07)62350-6.
[26] Peters LS, Brackmann EJ, Park WT. Future directions in automation and robotics for manufacturing. IEEE Aerosp Electron Syst Mag 1987;2:12–6. https://doi.org/10.1109/MAES.1987.5005320.
[27] Wierba EE, Finholt TA, Steves MP. Challenges to collaborative tool adoption in a manufacturing engineering setting: A case study. Proc Annu Hawaii Int Conf Syst Sci 2002;2002-Janua:3594–603. https://doi.org/10.1109/HICSS.2002.994456.
[28] Pardi T, Krzywdzinski M 1975-, Luethje B. Digital manufacturing revolutions as political projects and hypes: evidences from the auto sector 2020.
[29] Tao F, Qi Q, Wang L, Nee AYC. Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. Engineering 2019;5:653–61. https://doi.org/10.1016/J.ENG.2019.01.014.
[30] Jahromi AA, Kundur D. Fundamentals of Cyber-Physical Systems. Cyber-Physical Syst Built Environ 2020:1–13. https://doi.org/10.1007/978-3-030-41560-0_1/FIGURES/1.
[31] Cyber-Physical Systems - a Concept Map n.d.
[32] Bartocci E, Deshmukh J, Donzé A, Fainekos G, Maler O, Ničković D, et al. Specification-based monitoring of cyber-physical systems: A survey on theory, tools and applications. Lect Notes Comput Sci (Including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) 2018;10457 LNCS:135–75. https://doi.org/10.1007/978-3-319-75632-5_5/TABLES/2.
[33] Ali S, Qaisar S Bin, Saeed H, Khan MF, Naeem M, Anpalagan A. Network Challenges for Cyber Physical Systems with Tiny Wireless Devices: A Case Study on Reliable Pipeline Condition Monitoring. Sensors 2015, Vol 15, Pages 7172-7205 2015;15:7172–205. https://doi.org/10.3390/S150407172.
[34] Wang L, Törngren M, Onori M. Current status and advancement of cyber-physical systems in manufacturing. J Manuf Syst 2015;37:517–27. https://doi.org/10.1016/J.JMSY.2015.04.008.
[35] Calvaresi D, Marinoni M, Sturm A, Schumacher M, Buttazzo G. The challenge of real-Time multi-Agent systems for enabling IoT and CPS. Proc - 2017 IEEE/WIC/ACM Int Conf Web Intell WI 2017 2017:356–64. https://doi.org/10.1145/3106426.3106518.
[36] Chen Y. Integrated and Intelligent Manufacturing: Perspectives and Enablers. Engineering 2017;3:588–95. https://doi.org/10.1016/J.ENG.2017.04.009.
[37] Shaheen K, Hanif MA, Hasan O, Shafique M. Continual Learning for Real-World Autonomous Systems: Algorithms, Challenges and Frameworks. J Intell Robot Syst Theory Appl 2022;105:1–32. https://doi.org/10.1007/S10846-022-01603-6/METRICS.
[38] Kelechi AH, Alsharif MH, Ramly AM, Abdullah NF, Nordin R. The Four-C Framework for High Capacity Ultra-Low Latency in 5G Networks: A Review. Energies 2019, Vol 12, Page 3449 2019;12:3449. https://doi.org/10.3390/EN12183449.
[39] Zeb S, Mahmood A, Hassan SA, Piran MJ, Gidlund M, Guizani M. Industrial digital twins at the nexus of NextG wireless networks and computational intelligence: A survey. J Netw Comput Appl 2022;200:103309. https://doi.org/10.1016/J.JNCA.2021.103309.
[40] Xie J, Liu S, Wang X. Framework for a closed-loop cooperative human Cyber-Physical System for the

mining industry driven by VR and AR: MHCPS. Comput Ind Eng 2022;168:108050. https://doi.org/10.1016/J.CIE.2022.108050.
[41] San O, Rasheed A, Kvamsdal T. Hybrid analysis and modeling, eclecticism, and multifidelity computing toward digital twin revolution. GAMM-Mitteilungen 2021;44:e202100007. https://doi.org/10.1002/GAMM.202100007.
[42] Xu Y, Liu X, Cao X, Huang C, Liu E, Qian S, et al. Artificial intelligence: A powerful paradigm for scientific research. Innov 2021;2:100179. https://doi.org/10.1016/J.XINN.2021.100179.
[43] Alizadehsalehi S, Yitmen I. Digital twin-based progress monitoring management model through reality capture to extended reality technologies (DRX). Smart Sustain Built Environ 2023;12:200–36. https://doi.org/10.1108/SASBE-01-2021-0016/FULL/PDF.
[44] Phanden RK, Sharma P, Dubey A. A review on simulation in digital twin for aerospace, manufacturing and robotics. Mater Today Proc 2021;38:174–8. https://doi.org/10.1016/J.MATPR.2020.06.446.
[45] Qi Q, Zhao D, Liao TW, Tao F. Modeling of Cyber-Physical Systems and Digital Twin Based on Edge Computing, Fog Computing and Cloud Computing Towards Smart Manufacturing. ASME 2018 13th Int Manuf Sci Eng Conf MSEC 2018 2018;1. https://doi.org/10.1115/MSEC2018-6435.
[46] Qi Q, Tao F, Hu T, Anwer N, Liu A, Wei Y, et al. Enabling technologies and tools for digital twin. J Manuf Syst 2021;58:3–21. https://doi.org/10.1016/J.JMSY.2019.10.001.
[47] Lin C, Critchley P. Quantum Computing and Digital Twins 2022:199–214. https://doi.org/10.1007/978-3-031-04836-4_14.
[48] 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.
[49] Tariq U, Joy R, Wu SH, Mahmood MA, Malik AW, Liou F. A state-of-the-art digital factory integrating digital twin for laser additive and subtractive manufacturing processes. Rapid Prototyp J 2023. https://doi.org/10.1108/RPJ-03-2023-0113.
[50] Broy M. Engineering cyber-physical systems: Challenges and foundations. Complex Syst Des Manag - Proc 3rd Int Conf Complex Syst Des Manag CSD M 2012 2013:1–13. https://doi.org/10.1007/978-3-642-34404-6_1/COVER.
[51] Peter S, Vahid F, Gunes V, Givargis T. A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. KSII Trans INTERNET Inf Syst 2014;X:134–59. https://doi.org/10.3837/tiis.2014.12.001.
[52] Lee J, Bagheri B, Kao HA. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. Manuf Lett 2015;3:18–23. https://doi.org/10.1016/J.MFGLET.2014.12.001.
[53] Moller DPF, Vakilzadian H. Cyber-physical systems in smart transportation. IEEE Int Conf Electro Inf Technol 2016;2016-Augus:776–81. https://doi.org/10.1109/EIT.2016.7535338.
[54] Li Y, Sun D, Liu W, Zhang X. A service-oriented architecture for the transportation Cyber-Physical Systems. Chinese Control Conf CCC 2012:7674–8.
[55] Hou Y, Zhao Y, Wagh A, Zhang L, Qiao C, Hulme KF, et al. Simulation-Based Testing and Evaluation Tools for Transportation Cyber-Physical Systems. IEEE Trans Veh Technol 2016;65:1098–108. https://doi.org/10.1109/TVT.2015.2407614.
[56] Sampigethaya K, Poovendran R. Aviation cyber-physical systems: Foundations for future aircraft and air transport. Proc IEEE 2013;101:1834–55. https://doi.org/10.1109/JPROC.2012.2235131.
[57] Rao A, Carreon N, Lysecky R, Rozenblit J. Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems. IEEE Softw 2017;35:38–43. https://doi.org/10.1109/MS.2017.4541031.
[58] Kritzinger W, Karner M, Traar G, Henjes J, Sihn W. Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine 2018;51:1016–22. https://doi.org/10.1016/J.IFACOL.2018.08.474.
[59] Bottani E, Cammardella A, Murino T, Vespoli S. From the Cyber-Physical System to the Digital Twin: the process development for behaviour modelling of a Cyber Guided Vehicle in M2M logic n.d.
[60] Brenner B, Hummel V. Digital Twin as Enabler for an Innovative Digital Shopfloor Management System in the ESB Logistics Learning Factory at Reutlingen - University. Procedia Manuf 2017;9:198–205.

https://doi.org/10.1016/J.PROMFG.2017.04.039.
[61] Schleich B, Anwer N, Mathieu L, Wartzack S. Shaping the digital twin for design and production engineering. CIRP Ann 2017;66:141–4. https://doi.org/10.1016/J.CIRP.2017.04.040.
[62] Liu Y, Zhang L, Yang Y, Zhou L, Ren L, Wang F, et al. A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin. IEEE Access 2019;7:49088–101. https://doi.org/10.1109/ACCESS.2019.2909828.
[63] Karakra A, Fontanili F, Lamine E, Lamothe J. HospiT'Win: A predictive simulation-based digital twin for patients pathways in hospital. 2019 IEEE EMBS Int Conf Biomed Heal Informatics, BHI 2019 - Proc 2019. https://doi.org/10.1109/BHI.2019.8834534.
[64] Wan J, Yan H, Suo H, Li F. Advances in Cyber-Physical Systems Research. KSII Trans INTERNET Inf Syst 2011;5:1891. https://doi.org/10.3837/tiis.2011.11.001.
[65] Lee J, Azamfar M, Singh J, Siahpour S. Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing. IET Collab Intell Manuf 2020;2:34–6. https://doi.org/10.1049/IET-CIM.2020.0009.
[66] Park KT, Lee J, Kim HJ, Noh S Do. Digital twin-based cyber physical production system architectural framework for personalized production. Int J Adv Manuf Technol 2020;106:1787–810. https://doi.org/10.1007/S00170-019-04653-7/FIGURES/18.
[67] Russian cyberattacks pose greater risk to governments and other insights from our annual report - Microsoft On the Issues n.d.
[68] Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. vol. 54. Springer Netherlands; 2021. https://doi.org/10.1007/s10462-020-09942-2.
[69] Duo W, Zhou MC, Abusorrah A. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA J Autom Sin 2022;9:784–800. https://doi.org/10.1109/JAS.2022.105548.
[70] Chakraborty A, Alam M, Dey V, Chattopadhyay A, Mukhopadhyay D. Adversarial Attacks and Defences: A Survey 2018. https://doi.org/10.1145/nnnnnnn.nnnnnnn.
[71] Saghezchi FB, Mantas G, Violas MA, de Oliveira Duarte AM, Rodriguez J. Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs. Electron 2022, Vol 11, Page 602 2022;11:602. https://doi.org/10.3390/ELECTRONICS11040602.
[72] Zahid F, Funchal G, Melo V, Kuo MMY, Leitao P, Sinha R. DDoS Attacks on Smart Manufacturing Systems: A Cross-Domain Taxonomy and Attack Vectors. IEEE Int Conf Ind Informatics 2022;2022-July:214–9. https://doi.org/10.1109/INDIN51773.2022.9976172.
[73] Um D. Massive Sensor Array Fault Tolerance: Tolerance Mechanism and Fault Injection for Validation. J Robot 2010;2010:1–8. https://doi.org/10.1155/2010/745834.
[74] Metzen JH, Genewein T, Fischer V, Bischoff B. On Detecting Adversarial Perturbations. 5th Int Conf Learn Represent ICLR 2017 - Conf Track Proc 2017.
[75] Pei E, Ressin M, Campbell RI, Eynard B, Xiao J. Investigating the impact of additive manufacturing data exchange standards for re-distributed manufacturing. Prog Addit Manuf 2019;4:331–44. https://doi.org/10.1007/s40964-019-00085-7.
[76] Carchiolo V, D'Ambra S, Longheu A, Malgeri M. Object-oriented re-engineering of manufacturing models: A case study. Inf Syst Front 2010;12:97–114. https://doi.org/10.1007/s10796-008-9075-6.
[77] Gogolev A, Mendoza F, Braun R. TSN-Enabled OPC UA in Field Devices. IEEE Int Conf Emerg Technol Fact Autom ETFA 2018;2018-Septe:297–303. https://doi.org/10.1109/ETFA.2018.8502597.
[78] ECMA-363 - Ecma International n.d.
[79] Nasr ESA, Kamrani AK. Intelligent design and manufacturing. Collab Eng Theory Pract 2008:103–25. https://doi.org/10.1007/978-0-387-47321-5_6.
[80] About the Requirements Interchange Format Specification Version 1.1 n.d.
[81] ISO 14306:2017 - Industrial automation systems and integration — JT file format specification for 3D visualization n.d.
[82] NIST. IOT DEVICES AND INFRASTRUCTURES GROUP n.d.
[83] NIST. Model-Based Enterprise Summit 2014 n.d.

[84] NIST. Big Data at NIST n.d.
[85] NIST. CYBERSECURITY FRAMEWORK n.d.
[86] Shafto M, Conroy M, Doyle R, Glaessgen E. Modeling, Simulation, information Technology & Processing Roadmap. Technol Area 2010:1–32.
[87] Sharma A, Kosasih E, Zhang J, Brintrup A, Calinescu A. Digital Twins: State of the art theory and practice, challenges, and open research questions. J Ind Inf Integr 2022;30:100383. https://doi.org/10.1016/j.jii.2022.100383.
[88] Fuller A, Fan Z, Day C, Barlow C. Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE Access 2020;8:108952–71. https://doi.org/10.1109/ACCESS.2020.2998358.
[89] Githens G. Product Lifecycle Management: Driving the Next Generation of Lean Thinking by Michael Grieves. J Prod Innov Manag 2007;24:278–80. https://doi.org/10.1111/J.1540-5885.2007.00250_2.X.
[90] Phua A, Davies CHJ, Delaney GW. A digital twin hierarchy for metal additive manufacturing. Comput Ind 2022;140:103667. https://doi.org/10.1016/J.COMPIND.2022.103667.
[91] Vijayakumar K, Dhanasekaran C, Pugazhenthi R, Sivaganesan S. Digital twin for factory system simulation. Int J Recent Technol Eng 2019;8:63–8.
[92] Park KT, Nam YW, Lee HS, Im SJ, Noh S Do, Son JY, et al. Design and implementation of a digital twin application for a connected micro smart factory. Int J Comput Integr Manuf 2019;32:596–614. https://doi.org/10.1080/0951192X.2019.1599439.
[93] Liu C, Le Roux L, Körner C, Tabaste O, Lacan F, Bigot S. Digital Twin-enabled Collaborative Data Management for Metal Additive Manufacturing Systems. J Manuf Syst 2022;62:857–74. https://doi.org/10.1016/j.jmsy.2020.05.010.
[94] Konstantinov S, Hansen J de O, Assad F, Ahmad B, Vera DA, Harrison R. An analysis of the available virtual engineering tools for building manufacturing systems digital twin. Procedia CIRP 2023;116:570–5. https://doi.org/10.1016/J.PROCIR.2023.02.096.