Journal of Network and Computer Applications 245 (2026) 104373

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review article

Towards IT/OT integration in industry digitalization: A comprehensive survey

Riccardo Venanzi *, Giuseppe Di Modica, Luca Foschini, Paolo Bellavista

DISI - Dipartimento di Informatica Scienze e Ingegneria, University of Bologna, Viale Risorgimento, 2, 40136, Bologna, Italy

ARTICLE INFO

Keywords:
Industry 4.0
Industry 5.0
Communication and networking
IT/OT convergence
IT/OT integration
Cyber-physical systems
IIoT

ABSTRACT

According to both academic and industry perspectives, the Fourth Industrial Revolution has brought about a paradigm shift in the manufacturing sector enabling companies to enhance their competitiveness in the global market. To achieve this goal, manufacturing companies will need to undertake a deep digital transformation, primarily by introducing advanced Information Technology (IT) into traditionally less digitalized departments, such as shop floors, where Operational Technology (OT) currently dominate. For the full achievement of Industry 4.0 revolution objectives, practitioners believe in the strong requirement of a progressive and tight integration between IT and OT departments. In the depicted scenario, communication technologies are expected to play a pivotal role in facilitating the integration process, but other more recent and advanced IT have also proven helpful. In particular, the topic of IT/OT integration has attracted significant attention from various research communities that have sought to identify both the opportunities and challenges associated with its implementation. Although some good surveys of those works have appeared in the literature, to the best of our knowledge, no comprehensive review has yet been conducted that is fully dedicated to the topic of IT/OT convergence. In this paper, we propose a holistic approach to examine the various dimensions of IT/OT integration, which we classify into five interconnected realms, Communication, IT-Driven Support to OT, Human Centricity, Advanced Industrial Control Systems, and cybersecurity. Furthermore, we develop a realm-oriented taxonomy to organize the surveyed works in a structured manner, offering readers a clear overview of the current state of the literature, along with insights into unexplored opportunities and future directions for IT/OT integration.

Contents

* Corresponding author.
E-mail addresses: riccardo.venanzi@unibo.it (R. Venanzi), giuseppe.dimodica@unibo.it (G. Di Modica), luca.foschini@unibo.it (L. Foschini), paolo.bellavista@unibo.it (P. Bellavista).

https://doi.org/10.1016/j.jnca.2025.104373
Received 8 July 2025; Received in revised form 29 September 2025; Accepted 26 October 2025
Available online 4 November 2025

1. Introduction

Since the introduction of the term *Industrie 4.0*, which originated in Germany in 2011 (Industry, 0000), central and regional governments, standardization bodies, and research communities around the world have been sustaining and promoting a deep digitization of factories. Industrie 4.0 characterizes itself as a movement of innovative thoughts, ideas, and technologies aimed at revolutionizing the industrial sector.

The Industry 4.0 (I4.0) revolution calls for a paradigm shift that involves the extensive adoption of Information and Communication Technologies (ICTs) in all factory departments – from business operations to production lines – to radically transform production processes and the delivery of products and services. I4.0 fosters a deep change in the rigid organization model of the factory. The International Society of Automation (ISA) 95 (ISA, 0000) model characterizing the third industrial revolution imposed a hierarchical organization of departments, restricting interactions to within the same layer. With the advent of the fourth revolution, the ISA 95 pyramid is replaced by a flat organization, where boundaries between departments are blurred and smart "things" are free to interact in an *all-connected factory*.

Many standardization initiatives are independently contributing to the definition of architectural models where connected and interacting industrial objects will populate the factories of the future (IEC 62264-1:2013, 2020; RAMI, 0000; IIC IIRA, 0000; Wübbeke et al., 2017). In the envisioned landscape, a gradual yet decisive integration of the Information Technology (IT) and Operational Technology (OT) layers is anticipated. This process, commonly referred to as **IT/OT integration**, emphasizes the narrowing of both physical and conceptual gaps between the two domains. While IT focuses on managing and processing production data for business-oriented purposes, OT is dedicated to controlling physical processes and equipment. Historically, IT and OT have operated in isolation, with IT prioritizing scalability and interoperability, and OT emphasizing real-time control, reliability, and safety. This separation has led to limitations in their ability to support fully connected and intelligent industrial environments. Achieving the *all-connected factory* objective heavily relies on Communication Technologies (Cruz et al., 2016; Rao and Prasad, 2018; Time-Sensitive Networking (TSN), 2020; Nguyen-Hoang and Vo-Tan, 2019), both modern and legacy, which are tasked with providing the communication framework necessary for implementing IT/OT integration. Establishing a data path that bridges the boundary between IT and OT departments, or even extends beyond the company's borders, will enable innovative and profitable applications like *asset predictive maintenance* and *smart supply chain*. Together with Communication Technology, more recent and advanced Information Technology (Qi and Tao, 2019; Aazam et al., 2018; Liu et al., 2021; Antonino et al., 2022) has matured for adoption in OT-bound processes, establishing itself as a key enabler of the aforementioned integration. In such a challenging scenario, which envisions breaking down OT barriers in favor of a progressive convergence and integration of the OT and IT worlds, the surface for potential cyber-attacks expands significantly, emphasizing the urgent need for more robust mechanisms to ensure security of assets and safety of human workers as a top priority (Paes et al., 2020; Karampidis et al., 2019). With regard to humans, beyond the obvious emphasis on protecting the workforce in close contact with operating machines, there is significant interest within the research communities in evaluating the potential impact of human contributions on achieving integration goals (Huang et al., 2022; Carayannis et al., 2024; Castillo et al., 2021).

Recent literature surveys have highlighted research efforts that partially address the challenges and opportunities that arise from the integration of the IT and OT layers (ABB and Microsoft, 2019). Some tackle the topic of integration solely from the *communication* perspective, mainly addressing the contribution to the integration brought about by modern industrial communication protocols and standards (Ahmadi et al., 2018; Li et al., 2017; Aceto et al., 2019). Others have identified works that foster the convergence in layers above the communication one. Among these, Raptis et al. (2019) and Wortmann

et al. (2017) point out the importance of *data management strategies and models* to fulfill industrial needs such as smart maintenance, prognostic, anomaly detection, and task scheduling. In Qi and Tao (2018), authors stress the boost given by the Big Data and Digital Twins paradigm towards the realization of strong integration of factories' business and operational departments. Some works collected and analyzed research contributions asserting that the foundation for IT/OT integration must be established at the shop floor level, through the modernization and digitization of physical assets that implement industrial control (Hofer, 2018; Xu et al., 2018). Finally, there are a number of literature surveys that deal with *security concerns* raised when the physical and cyber world integrate (Figueroa-Lorenzo et al., 2020; Bhamare et al., 2020). The reader may refer to Section 5 for a comprehensive and detailed review of literature surveys on the topic of IT/OT integration.

Despite the abundance of surveys in recent literature, to the best of our knowledge, no effort comprehensively explores the implications of IT and OT integration within modern industry. Unlike previous surveys, in this work we adopt a rigorous and systematic approach that drives the reader through the many facets of integration opportunities and issues. Firstly, we provide insights on the historical and technological landscape upon which this integration is grounded. Secondly, inspired by the depicted context, we devise a taxonomy that helps us categorize all surveyed works and identify their contribution to the integration topic along specific dimensions of the problem. According to the taxonomy structure, a relevant number of literature proposals address integration at the **Communication** layer, others propose to favor the convergence of IT/OT with solutions supported by the most recent and advanced IT (see **IT-driven support to OT**), while some contribute to the discussion with works targeting **Advanced Industrial Control Systems**. The proposed taxonomy also includes a *Cybersecurity* category, which encompasses contributions addressing security and safety challenges emerging from IT/OT integration, as well as a branch dedicated to works focusing on *Human-centric* aspects. Finally, based on the results of the conducted study, we provide the reader with a synoptic view of the state of the art and delineate future directions. It is important to note that, in this paper, the term *convergence* refers to the process that leads to the integration of IT and OT within the Industry 4.0 landscape. Given the close affinity between the two concepts, the terms *integration* and *convergence* will be used interchangeably throughout the remainder of the paper.

Fig. 1 depicts the structure and organization of the paper. In Section 2, we illustrate the review methodology that guided the review of the literature. In Section 3, we provide a thorough description of the research background. In Section 4, we propose an analysis of the I4.0 standardization initiatives in the perspective of IT/OT convergence. In Section 5, we review the recent literature and motivate the need for this survey. In Section 6, we introduce the taxonomy adopted to frame and structure the body of literature in the field. Sections 7, 8, 9, 11 and 10 deep dive into all taxonomy branches. In Section 12, we discuss the results of the research conducted and give an overview of the investigation areas. Finally, we conclude the work in Section 13.

2. Research method

This section outlines the research method that was used to carry out the systematic literature review presented in this work. The purpose of the paper is to provide the reader with a clear understanding of the problem and to identify the most urgent directions for research on IT/OT convergence in modern industry. The four-step process developed to achieve that objective is described below.

Review of recent literature. This step focuses on gathering works published in the last decade and a half that address the various aspects of IT/OT integration. Initially, we concentrated on survey papers, i.e., works that, like ours, aim to collect and classify existing research and proposals related to IT/OT convergence. This twofold strategy allowed us to (i) reconstruct the landscape of studies connected to our work and (ii) collect references to the underlying research proposals. After analyzing existing surveys, we extended the review to include research contributions not cited in prior surveys. In order to identify the scientific works most relevant to our objectives, a search was conducted across the major publishers and indexing platforms (Scopus, Google Scholar, ACM Digital Library, IEEE Xplore Digital Library, Elsevier ScienceDirect, SpringerLink, etc.), using the keywords "IT/OT integration" and "IT/OT convergence". Given that the digital transformation in the industrial domain is generally recognized to have begun around fifteen years ago (Industry, 0000), all works published before 2010 were excluded from the analysis.

Review of standardization initiatives. This step consisted in reviewing all main industrial standardization efforts, at both national and international levels. These initiatives are particularly relevant, as they define the guidelines and roadmaps that shape and accelerate the digital transformation of the modern industry. The objective of this step is to gather widely recognized insights from international standardization bodies in order to establish a theoretical foundation for the conceptual framework to be defined in the subsequent phase.

Designing of a conceptual framework. Building on the collected material, we introduced a systematic approach to the problem of IT/OT integration by defining a comprehensive taxonomy. The taxonomy, structured into *realms* and *branches*, provides an organizing framework to categorize and interpret contributions retrieved from the literature, thereby serving as the conceptual backbone of our study.

Outlining directions for future research. Building on the systematic literature review conducted in the previous step, this phase involved a synthesis aimed at producing a synoptic overview of the main research activities carried out across the various realms of IT/OT integration, as well as highlighting those areas of integration that remain insufficiently explored.

3. The narrowing gap between OT and IT in modern industrial control systems

In this section, we provide an overview of the basic components and technology of the industrial process automation and delve on how the latter is expected to evolve in the light of the new directions indicated by the fourth revolution.

Automation of industrial production is one of the fundamental mandates of the third industrial revolution. Industrial Control Systems (ICSs) were pivotal in driving such automation. ICSs are computerized systems used to monitor and control industrial processes, machinery, and infrastructure in sectors such as manufacturing, energy, transportation, and utilities. ICSs receive data from remote sensors measuring industrial process variables, compare the collected data with desired set points, and trigger command functions to control the process through the final control elements, such as valves. In the following, we explore the technological background that ICSs are built upon, discuss the evolution pattern of modern ICSs and dwell on the technology integration process that enables and supports such evolution.

ICSs are at the core of Operational Technology (OT) departments. OT mainly concerns with mechanical assets within production facilities mapped on the lower layers of pyramidal structure of automation presented and standardized by ISA95 (Foehr et al., 2017). According to Gartner (When IT, 0000), *...OT is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events...*. OT supports the implementation of closed-loop control of working machines through "vertical" (i.e., tightly-coupled) HW/SW systems that leverage sensors/actuators deployed in the proximity of machines. In such systems, both sensed data and control signals travel on protected and reliable industrial networks that guarantee high data throughput and very low communication latency as requested by real-time and computation-intensive

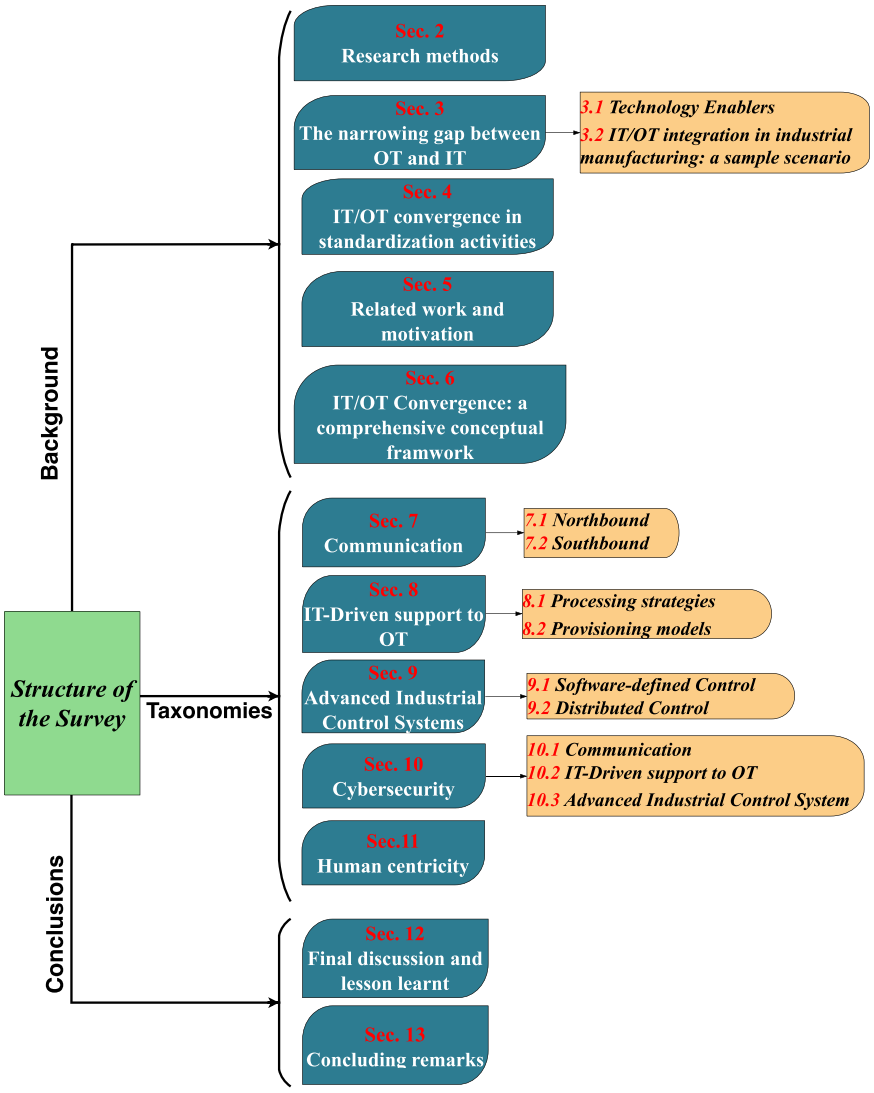

Fig. 1. Paper structure.

tasks that control the production process. Furthermore, as human workers operate in close contact with the production machines, machine faults that might compromise workers health must be predicted and corrected in an timely way. The *task-specific* nature of OT systems and their employment in mission-critical domains have historically overshadowed innovation and interoperability (that are instead fundamental features of IT-centric systems) in favor of reliability, robustness, and workers' safety.

Key components of an OT system include: *Supervisory Control and Data Acquisition (SCADA)*, used to monitor and control industrial processes and collect real-time data from sensors, devices, and machines; *Programmable-Logic Controllers (PLCs)*, industrial processor adapted for the control of production processes, such as assembly lines, machines, robotic devices, etc.; *Remote Terminal Units (RTUs)*, devices that interface with sensors and other equipment in the field and transmit the data back to a central control system; *Industrial Networks (INs)*, connecting the various components of an ICSs and allowing them to communicate and exchange data (common industrial network protocols include Modbus, Profibus, and Ethernet/IP); *Distributed Control Systems (DCSs)*, similar to SCADA systems but typically used for more complex and larger-scale industrial processes.

In the hierarchical and rigid vision of the ISA95 automation pyramid, Information Technology (IT) mostly occupy the top two layers. *IT* deal with gathering, storing, and analyzing data produced by work machines in the *shop floor*. IT embraces applications, frameworks, and telecommunication assets that support the management of enterprise resources/data and business activities. Historically, in the IT layers service requirements have been more relaxed than in OT. Data processing occurs offline and is usually accomplished by means of software tools like Manufacturing Execution Systems (MES), Manufacturing Operations Management (MOM) and Enterprise Resource Planning (ERP) (ISA, 0000). MES enable the monitoring of raw materials and production processes, improving plant performance and containing management costs. ERP aims to optimize the business performance of the company by providing support to plant scheduling, supply chain management, inventory maintenance, and customer services provisioning. MOM systems communicate with ERP and translate production orders into commands for operators, machinery, and assembly lines, with a focus on optimization efficiency. Nowadays, MOM and ERP tend to be more interlaced (Li et al., 2020) and encompass new analysis tools equipped with Artificial Intelligence (AI) capabilities in order to face the lack of flexibility and boost the adaption to new business needs and models.

The clear IT/OT separation is a strong founding principle of ICSs. In spite of the many advancements done by emerging IT in non-industrial sectors – of which agile/interoperable communication protocols and flexible computing paradigms are just a few examples – industry practitioners have refrained from largely adopting such technologies in the

lower layers of the pyramid, mainly because of the impact that such adoption could generate on the system's robustness, reliability, and security. In the last decade, the flourishing of cultural and technological initiatives is driving a new industrial revolution that, leveraging the extraordinary evolutionary path of IT, is fostering a new concept of factory better known as "all-connected factory". According to this vision, the progressive penetration of IT into the OT environments neatly split the ISA95 pyramid in more flattered structure where industrial assets (sensors, machines, production lines, business processes) are fully integrated with IT layers and virtually capable of interacting with each other across all factory layers (RAMI, 0000). In the prospected framework, IT is expected to provide additional functionality and services to support the management of ICSs. In that regard, key aspects are considered:

- **Network infrastructure**. This includes the possibility of establishing wired or wireless connections, configuring routers and switches, and ensuring reliable and secure communication between industrial devices, processes, etc.
- **Remote Monitoring and Control**. IT enables remote monitoring and control of industrial assets/processes by leveraging technologies such as Cloud Computing and the IoT.
- **Data management.** IT enables the (real-time) collection, storage, analysis, and visualization of data generated by industrial processes. Such enhanced capability of handling data will serve the purpose of monitoring and optimizing industrial operations, and facilitates the integration of operational data with the business systems for decision-making such as, e.g., predictive maintenance of shop floor machines, design of a resilient and robust supply-chain.
- **Legacy System Integration.** Legacy OT environments often rely on proprietary protocols, rigid architectures, and physically isolated networks, limiting interoperability and scalability. IT introduces standardized communication frameworks, middleware solutions, and secure IP-based networking to seamlessly connect legacy systems, and sensors with cloud platforms, AI analytics, and enterprise IT systems.
- **Cybersecurity**. It refers to the availability of robust security measures (such as firewalls, intrusion detection systems, etc.) to protect the production environment against unauthorized access, data breaches, and other correlated risks.

The penetration of IT into OT is progressing steadily but surely. A clear example of this evolution can be seen in SCADA systems, which have undergone three distinct generations. This evolution is slowly turning the traditional ICS in Cyber Physical Systems (CPS) over time (Rajkumar et al., 2010; Lee and Seshia, 2017; Alur, 2015). CPS, in industrial context, are advanced systems that integrate computational algorithms with physical industrial processes. They use sensors, actuators, and communication networks to monitor, control, and optimize operations in real time, enabling seamless interaction between digital technologies and physical machinery. CPS are central to modern industrial innovations like smart factories, predictive maintenance, and real-time process optimization (Shi et al., 2011; Cogliati et al., 2018; Jiang, 2017). The mentioned evolution is replacing isolated, deterministic control with interconnected systems leveraging IoT, AI, and Cloud/Edge computing for real-time decision-making and adaptability. The result is a flexible, scalable industrial environment that enhances efficiency, predictive maintenance, and security, enabling smart factories and Industry 4.0. This transformation is further explained and addressed in Section 9.

The technologies and the paradigms which concretely enable the integration of IT and OT worlds are deepened in the following section, while in the next one we present a real example of the potential benefits brought by the IT/OT integration in the modern factory.

3.1. Technology enablers

The integration of IT and OT layers in industrial systems is enabled by a range of emerging technologies and methodologies. This section presents a non-exhaustive list of key enablers, organized chronologically by their appearance, that support the integration scenarios envisioned by Industry 4.0. The discussion covers computing paradigms, methodologies, and specific technologies that facilitate this convergence. Fig. 2 provides a synthesized overview of these enablers along with their principal features that contribute to the integration objective.

Cloud Continuum (CC) (Qi and Tao, 2019; Jiang and Wan, 2021) is a novel compute provisioning paradigm that seamlessly integrates and combines benefits of various technologies such as Cloud, Fog, and Edge Computing with IoT nodes. This continuum allows industries to leverage the best aspects of each layer—scalability, low latency, and control—based on their specific needs. CC is emerging as a revolutionary paradigm for industrial operations that sustains seamless integration of IT and OT layers. On the one hand, Cloud Computing meets many industrial production requirements by providing on-demand services, great scalability, a pay-per-use model, available resources sharing, accessibility through broad network access. By leveraging the flexibility, data centralization, connectivity, security, and collaboration benefits of Cloud Computing, organizations can achieve enhanced operational efficiency and improved decision-making capabilities, thus unlocking the full potential of IT/OT integration (Pittalà et al., 2024). The central control plane provided by the cloud improves the coordination between IT and OT components, supporting holistic and integrated operations. Cloud Computing also encourages the adoption of software development paradigms (e.g., Service Oriented Architectures(SOA) Niknejad et al., 2020; García-Domínguez et al., 2013), communication protocols (REST, MQTT Mqtt, 0000, AMQP Amqp home, 2008), and virtualization practices (for both computing resources Queiroz et al., 2023 and network infrastructures Chi et al., 2022) that are expected to streamline the integration process and promote better alignment between IT and OT objectives. On the other hand, industrial Edge/Fog computing models (Aazam et al., 2018) focus on positioning computational resources as close to data sources as possible. In production environments, they offer significant enhancements to cloud-based smart manufacturing processes. In IT/OT converging networks, the vast amounts of data generated by sensors and devices can make cloud transmission expensive and inefficient. The additional layer introduced by Edge/Fog brings highly sought-after capabilities such as real-time data processing and agile decision-making, made possible by the low latency and high throughput inherent to these architectures. These compute provisioning models offer a scalable and adaptable architecture, allowing edge devices or fog nodes to be deployed effortlessly to meet evolving requirements without the need for significant infrastructure modifications. The "local" processing also strengthens cybersecurity, as sensitive industrial data remains within the local network, minimizing exposure to external threats and ensuring compliance with strict security and privacy regulations.

Modern **IIoT protocols** are by many believed to play a central role in building the pathway to the IT/OT integration (Bosi et al., 2020; Stratogiannis and Gkiala-Fikari, 2018; Nguyen-Hoang and Vo-Tan, 2019). With the development and deployment of applications based on IIoT protocols, companies can build their own bridge between IT systems and OT equipment endpoints. IIoT protocols enable the interoperability between different devices, systems, and applications in both IT and OT domains providing standardized ways for devices and systems to communicate and share data, regardless of the underlying technologies and platforms. Furthermore, the employment of pub/sub messaging pattern allows for real-time and event-driven communication, making it well-suited for capturing and responding to operational needs in industrial settings. The Message Queuing Telemetry Transport (MQTT) (Mqtt, 0000) protocol is a lightweight, highly-scalable publish/subscribe messaging protocol, built on top of the

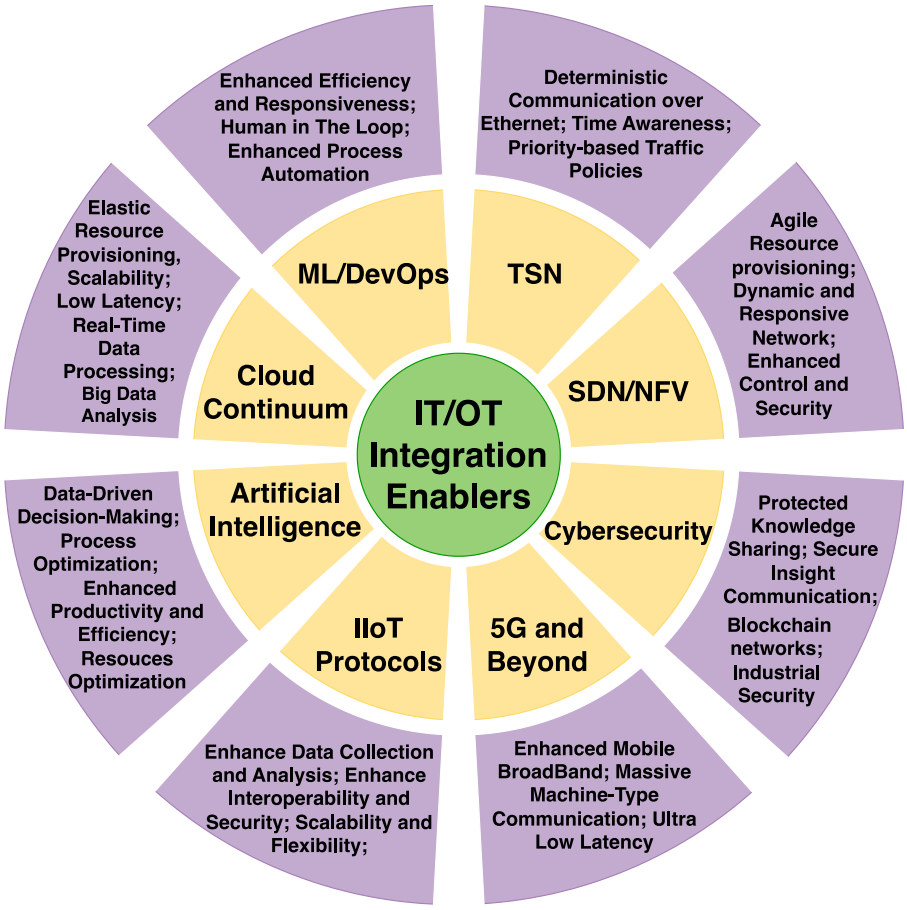

Fig. 2. ICT technologies enabling the integration.

TCP/IP stack, based on the hierarchical topic definition. It offers different quality of service policies for messaging delivery. Advanced Message Queuing Protocol (AMQP) (Amqp home, 2008) is another well-known application-layer IIoT protocol that provides interoperability in the IT/OT integration industry by defining a common schema for representing a wide range of commonly-used application types. The performance and reliability of message delivery make this protocol fit many industrial use cases such as monitoring resources and integrating legacy systems. Constrained Application Protocol (CoAP) (Coap home, 0000) is a web-transfer, REST-based protocol built on top of UDP that enhances the network performance of constrained devices. With its versatile integration capabilities and diverse implementations addressing various use cases, the CoAP protocol is well-suited for connecting IT and OT layers in industrial environments. OPC Unified Architecture (UA) (OPC UA) (Unified architecture, 2019) is one of the main platform-independent protocols employed in the shop floor for the communication of work machines through both Client/Server and Pub/Sub models. OPC UA offers robust authentication and cybersecurity mechanisms thus serves as a de facto standard in modern IT/OT integration scenarios.

Software-Defined Networking (SDN) and **Network Function Virtualization (NFV)** enable easy and flexible management of communication networks, providing agility and end-to-end control over industrial infrastructure deployments (Cruz et al., 2016; Shrestha and Lin, 2020; Yannuzzi et al., 2017). By leveraging the SDN paradigm, companies will progressively abandon the IT and OT silos approach in favor of an integrated common networking environment. SDN is expected to supersede VPN-based mechanisms, that are known to introduce non-negligible latency and hinder the management of resources in full autonomy. Network segmentation offered by SDN will allow companies to carry out agile provisioning of enterprise-level services that are requested in modern industrial scenarios. NFV provides Virtual Network Functions (VNF) that enhances the reliability and robustness of currently operating services and hides away the complexity of managing the underlying network. When employed in synergy, SDN and NFV allow organizations to build more dynamic, adaptable and responsive networks that can support the integration of IT and OT systems (Kupzog et al., 2020). For instance, the combination of SDN and NFV enables the creation of virtual network segments that can be dedicated to specific OT applications, providing better control and security (Mamduhi et al., 2022). Both IT and OT departments can deploy network services on existing Commercial Off-The-Shelf (COTS) hardware without dedicated network assets, thus making a step forward to a reliable integration of the two worlds.

The recent advancement of software analysis leveraging **Artificial Intelligence (AI)** techniques has facilitated their adoption in production plants (Ameri et al., 2024; Deng et al., 2022). Plant and product analysis are crucial enablers of many widely used AI-based features provided by IT/OT integration, such AD, PM, ZDM. In this context with AI/ML techniques we mean all AI-driven and learning-oriented approaches, spanning from ML to Reinforcement Learning, including Federated Learning, Deep Learning, Distributed Learning, etc. Integrating AI/ML techniques into IT/OT systems allows organizations to harness real-time data from operational processes for data-driven decision-making and performance optimization (Liu et al., 2021). These techniques can help uncover patterns, anomalies, and correlations that traditional analytics might miss. By continuously analyzing data and feedback, AI/ML algorithms can adjust system parameters, optimize processes, and enhance overall performance over time. This adaptability is especially valuable in dynamic IT/OT convergent industrial

environments where conditions and requirements may change frequently. AI/ML enable predictive and prescriptive analytics, which are crucial for proactive maintenance, quality control, defectiveness control, waste control, and operational optimization (Gahlawat et al., 2023; Hicham et al., 2023). Furthermore, in IT/OT convergent networks, AI/ML approaches, i.e. federated learning ones, can enhance cybersecurity by detecting and mitigating threats in real-time, helping the improvement of the resilience and security of IT/OT infrastructure (Bhamare et al., 2020; Anjum et al., 2025; Belenguer et al., 2023; Nuaimi et al., 2023).

IT/OT integration necessitates a modern **cybersecurity** approach, primarily to safeguard work stations from external threats (Paes et al., 2020; Bhamare et al., 2020). Industrial environments face a growing number of cyber threats, including malicious attacks, ransomware, and unauthorized access. Strengthened cybersecurity measures are essential to safeguarding critical infrastructure, systems, and sensitive data against these risks. In the modern IT/OT paradigm, operations and processes depend on key assets such as control systems, industrial machinery, and network infrastructure. A breach of these assets can lead to serious repercussions, including production downtime, safety risks, and financial losses. Comprehensive cybersecurity strategies protect these assets through measures such as access controls, network segmentation, intrusion detection systems, and encryption. Beyond access control, cybersecurity plays a critical role in monitoring machine-to-machine communications and detecting anomalies that may arise in automated exchanges. Such deviations can indicate potential attacks aimed at causing unintended machine behavior, which could ultimately result in hazardous situations for workers (Karampidis et al., 2019). Implementing cybersecurity policies could require collaboration between IT and OT teams, who are thus encouraged to share knowledge and efforts to identify and mitigate potential security risks. In the past few years, many have employed blockchain networks in order to improve IIoT features (Huo et al., 2022). The decentralization, non-repudiation, and reliability of blockchain networks bring powerful features to IIoT-connected devices by adding distributed secure storage, non-tampering proofs, decentralized collaborative manufacturing, and efficiency in access control.

The spread of modern cellular networks, such as the **5G and beyond-5G** technologies (Rao and Prasad, 2018; Ghildiyal et al., 2023), will offer companies a powerful and reliable radio communication means to support processes that require communication latency in the order of milliseconds as well as a complete coverage of the factory premise. The 5G networking supports three communication modes potentially suitable for industrial production scenarios: enhanced Mobile BroadBand (eMBB), massive Machine-Type Communication (mMTC), and Ultra-Reliable Low-Latency Communications (URLLC) (Pei et al., 2025). Modern cellular networks provide a ubiquitous and reliable wireless communication infrastructure that can connect a variety of devices and systems, facilitating the seamless integration of IT/OT layers within firms. The ensured high bandwidth and low latency are essential for OT applications, enhancing operations and enabling faster decision-making in the IT layers (Ambrosy et al., 2022). The security of modern cellular networks is improved with encryption and authentication mechanisms to protect data and prevent unauthorized access, ensuring the safety and security of critical systems. The scalability and flexibility of mobile networks allow them to easily adapt to the changing needs of IT and OT systems, enabling quick and efficient deployment of new applications and services and scaling the IT/OT infrastructure as needed. Additionally, the network slicing feature introduced by 5G will support the coexistence of multiple data flows with diverse timing requirements, which is a key requirement for the integration of OT and IT systems (Afolabi et al., 2018).

The deterministic features of the **Time-Sensitive Networking (TSN)** standards (Time-Sensitive Networking (TSN), 2020) will play a key role in enabling successful IT/OT integration within production facilities. TSN technology is considered a critical enabler of this integration, as it facilitates seamless interaction between IT and OT assets. While IT systems typically use standard Ethernet communication, OT systems demand real-time communication with stringent timing requirements, which TSN effectively supports. TSN grants deterministic communication over Ethernet by introducing different traffic flows sharing the same physical link. Time awareness of TSN protocols enables real-time capabilities that operational assets in production plants need, while keeping the benefits of best-effort communications used for the purpose of typical IT tasks like offload information processing (Khona, 2017). The filtering policies regulate the priority of the packets at every layer, whereas the network configurations (Central Network Controller or CNC and Centralized User Configuration or CUC) allow scheduling for transmissions and receptions, by enabling a reliable and fine-grained configurable communication path inside converging environments.

In Industry 4.0/5.0 settings, **DevOps** (Antonino et al., 2022) (Development and Operations) and **MLOps** (Faubel et al., 2023) (Machine Learning Operations) are gaining momentum as methodologies that enhance efficiency and responsiveness of dynamic industrial processes. DevOps is a typical IT collaborative approach that, in a modern industrial environment, integrates software development and operational technology teams to automate and optimize the deployment, monitoring, and maintenance of industrial systems, improving efficiency, reliability, and real-time responsiveness. MLOps, a specialized extension of DevOps, addresses the challenges posed by integrating machine learning into production environments. It focuses on operationalizing machine learning models, automating processes related to training, testing, deployment, and monitoring. In Industry 4.0, where data-driven decision-making is crucial, MLOps ensures seamless integration of machine learning models to optimize tasks like predictive maintenance and quality control. Combined, DevOps and MLOps create a powerful framework that enhances the efficiency, agility, and responsiveness of industrial processes by streamlining software development, deployment, and the integration of machine learning models.

Finally, the following sub section presents a concrete modern industrial scenario in which the integration of IT/OT layers plays a pivotal role and most of the described enablers are involved.

3.2. IT/OT integration in industrial manufacturing: a sample scenario

Since the advent of the third industrial revolution, data from industrial production lines have gained increasing relevance with a view on cost cutting, production processes optimization, and increase of revenues (Zawra et al., 2019). Traditional industrial deployments are used to keep the worlds of automation (OT layer) and ICT services (IT layer) isolated, with no or few chances of interactions. This practice hinders the companies from fully exploiting the real potential of production data, effectively renouncing to maximize the efficiency of production processes, minimize energy consumption, rationalizing man–machine time, and the improving the quality of the human operator's work.

In traditional industrial manufacturing settings, companies are used to adopt old and ineffective machine maintenance procedures (LLC, 2021). Many production plants rely on reactive, run-to-fail maintenance processes, i.e., they perform repairs only after equipment has broken. This approach proved inefficient, because it triggers unplanned machine downtime that eventually cause waste of money to the company. In order to mitigate such inefficiencies, companies started adopting practices that mainly leverage historical machinery data or machine data sheets for scheduling periodical repairs, thus preventing potential breakages (hence the term *preventive maintenance*) and prolonging the assets' lifespan. In spite of the benefits brought by the preventive approach, manufacturers still have to invest time and resources for periodically repairing equipment, independently of its actual remaining useful life, which anyway does not provide strong guarantees of avoiding breakage and production downtime. Forbes reports 82% of companies have experienced at least one unplanned downtime incident over the previous three years. Such a problem is estimated to costs

industrial manufacturers $50 billion per year. In the case of automotive industry, manufacturers lose on average $22,000 per minute when the production line stops (LLC, 2021; LLC., 2022). Another serious issue in the industrial manufacturing sector is the inability of companies to detect the degradation of product quality in a timely manner. Not being able to detect potentially defective products may cause a waste of raw material, production line capacity, and workforce time. Last but not least, it has a huge impact on the environment in terms of, e.g., waste of electricity and pollution due to disposal of the defective product.

In the two depicted scenarios, the lack of accurate and timely information on crucial production process variables (such as the actual state of health of machinery and the compliance of the work piece with the product layout) prevent companies from taking effective counteractions that could effectively mitigate the process performance degradation. IT offer to manufacturing companies the opportunity to build such information. With regards to the machine maintenance scenario, sensors can be placed near the machinery to monitor data related to the machinery's health and continuously transmit this information from the shop floor to computing premises (e.g., Fog/Cloud). To support the data shipment process, robust and mature technologies like the SDN/NFV can be leveraged that enable the quick set-up and easy operation (e.g., real-time adjustments to network configurations to prioritize anomaly detection signals) of a common network infrastructure spanning both OT and IT; on top of that infrastructure, standardized, industry-oriented communication protocols like the OPC UA will guarantee a reliable, timely and end-to-end data transport. Once they have reached the destination, the collected (Big) data are used to train ML/DL models capable of detecting anomalous behaviors of wearing parts, thus predicting potential upcoming breakages with a certain level of confidence. Should the anomaly detection have mission-critical requirements, the predictive models could be set to run close to the machine premises (e.g., on Edge devices), so to minimize the communication delay between the sensors and the models that consume the sensed data. By combining fresh insights on the machinery health with machinery's historical production data, the company will be able constantly monitor the machinery's remaining useful time and devise more precise and sustainable maintenance plans. The discussed maintenance scenario implements two innovative and well-known industrial practices known as Anomaly Detection (AD) and Predictive Maintenance (PM) respectively. AD is employed to detect at run-time anomalous behaviors in the production process or, as discussed above, in the industrial asset, thus allowing the company to promptly adjust deviations from the production target. PM is a technique that employ both historical and production machinery data to evaluate the current health state and alert the operator before a failure occurs (Bellavista and Di Modica, 2024).

In a similar way, the *product optimization scenario* could take advantage of the mentioned ITs (IIoT, Big Data, AI, Cloud/Edge, SDN/NFV) to enforce fine-grained control over the production quality. In the literature, the methodology that aims to achieve a defect-free production process is referred to as the Zero Defect Manufacturing (ZDM) (Caiazzo et al., 2022; Venanzi et al., 2023a). ZDM is a novel approach to manufacturing that exploits AD and PM techniques, along with DT and DevOps, to implement defect-free production processes. More in detail, ZDM exploits the DT-based techniques to reproduce the machinery and process in virtualized environments; then, prediction of anomalies and/or failures is achieved through AD and PM algorithms. Once an anomaly, defect, or failure is predicted, new settings and process configurations can be deployed to the real machine to counteract process deviations, utilizing DevOps practices. ZDM achieve extremely high-efficiency production processes, by tearing down wastes and maximizing company profits. To summarize, the convergence of IT/OT layers fills the gap between a massive amount of data generated by the industrial assets/processes and their actual full exploitation. In the proposed scenario, it enables AD, PM, and ZDM techniques which boost the efficiency of production lines, minimize the wastes, and prevent financial losses for the company by exploiting advanced monitoring, digital twinning, and ML/DevOps procedures.

4. IT/OT convergence in standardization activities

In the past decade, various countries have launched standardization initiatives addressing the business and technological aspects of the Industry 4.0 transition. These initiatives are helping to facilitate the successful IT/OT convergence process, which is seen as a prerequisite for the transition. In this section, we will briefly introduce the most authoritative initiatives and examine the specific standards that address the convergence topic.

The European Reference Architectural Model Industrie 4.0 *RAMI 4.0* (RAMI, 0000) proposes a structured approach to the development of an I4.0 platform. Not only RAMI 4.0 fosters a higher degree of interaction between OT and IT departments; it also promotes the opening of enterprises' boundaries to better sustain the business objectives. In such perspective, IT will play a pivotal role. The model develops on a three-dimensional map, depicted in Fig. 3, structured as follows:

- *Hierarchy level*. This dimension provides a functional description of components acting in the factory, such as field and control devices, stations, work centers, and the enterprise as a whole. The last element in this axis is the Connected World, that underlines the importance of extending the factory environment to the external world.
- *Life cycle & value stream*. This is the key axis focusing on the whole production cycle of a smart product, and it describes the current lifetime point and location of an object. This layer is also a key connection point between enterprises, in the sense that a product in Instance phase in a company could be an input to the Type phase of a product in another company. This aspect helps the enterprises to identify interconnections and dependencies of a product with respect to other companies.
- *Layers*. This dimension provides the classic layered approach to the design of the IT architecture that facilitates the development of novel solutions by splitting complex technological issues into smaller and simpler problems.

In particular, the *Layers* axis remarks the central role of corporate assets by defining the *I4.0 Component* concept, an interactive entity representing a physical asset in the digital world capable of exchanging data with both intra- and inter-factory business processes. Through the Layer axis, RAMI proposes an architectural view of the factory digitization process, as outlined in Fig. 4. The RAMI perspective tears down the barriers that take IT and OT apart, and fosters a progressive integration of physical assets into the digital world where they are expected to provide enhanced economic value for all the stakeholders. In the RAMI view, key aspects of the convergence process are the digitization of physical assets (via the *Integration layer*) and the *Communication layer* among I4.0 Components.

With the Made In China (MIC) 2025 initiative (Wübbeke et al., 2017), inspired by the Germany's I4.0, China formalized its 10-year industrial plan for the 10 most important production sectors in the region. The strategy focuses on the implementation of smart manufacturing techniques improving efficiency, quality and productivity inside the factory's shop floor. As the actuation of the initiative envisions enhanced interconnection and factory digitization, information technologies and IoT play a crucial role to connect SMEs production chains with the global production network. The target of the plan is the whole production industry, including all stakeholders, from technical to managerial departments, whereas the demand is the formalization and the adoption of international technical standards.

In this context, the committee defined the Intelligent Manufacturing System Architecture (IMSA) specification. IMSA is a framework that provides a structured approach to integrating advanced technologies into manufacturing systems. It emphasizes interoperability, modularity, and scalability to enable efficient, flexible, and intelligent production processes. By leveraging technologies such as IoT, AI, and real-time

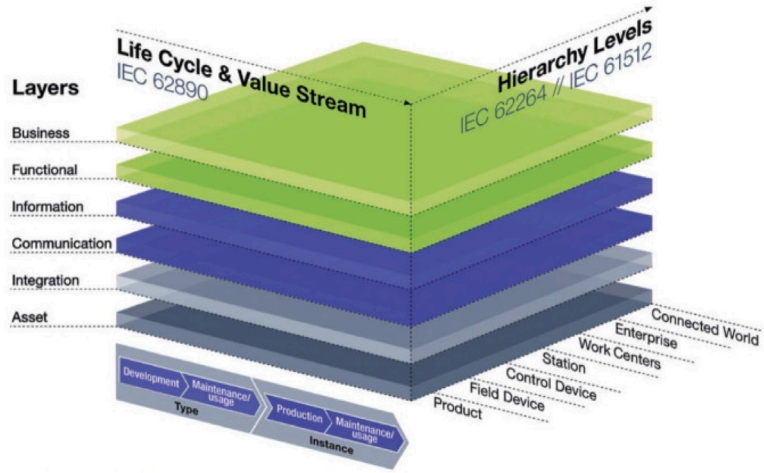

Fig. 3. The RAMI 4.0 reference architectural model.
Source: Platform Industrie 4.0.

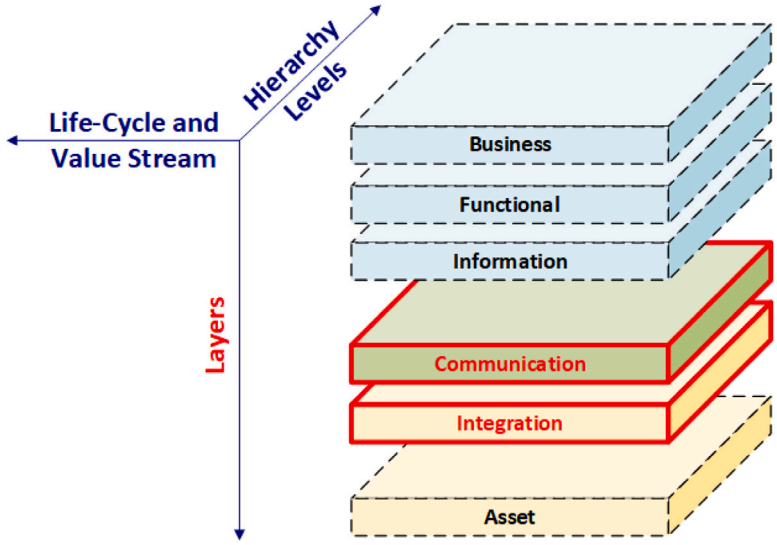

Fig. 4. IT/OT convergence in RAMI 4.0.

data analytics, IMSA supports the seamless coordination of resources, systems, and workflows to optimize manufacturing operations and adapt to dynamic market demands.

The three-axes reference model is substantially similar to the RAMI 4.0. The *lifecycle* axis refers to value creation activities, covering the whole life of a product. The *system hierarchy* axis identifies the entities involved in the manufacturing process through five layers: equipment, control, workshop, enterprise and cooperation. The *intelligent functions* axis identifies the smart manufacturing functions that need to be implemented within the factory, such as self-sensing, self-adaptation, predictive maintenance, accomplished through the exploitation of modern information and communication technologies. The IMSA architecture aims for cross-boundary integration in the intelligent manufacturing sector.

As shown in Fig. 5, with focus on the *Intelligent Functions* axis of the three-axes architecture, the *Interconnection* and *System Integration* layers are responsible for the integration and connection of the industrial asset with the control and management enterprise software. With that vision, the ambition of the MIC initiative is to harmoniously integrate into the same loop the complex IT business processes of control and management of the plants with the hardware technologies of the OT domain.

The American *Industrial Internet Reference Architecture (IIRA)* initiative (IIC IIRA, 0000) promotes the *Industrial Internet* concept to bring industrial control systems online, so as to form large end-to-end systems connected with people and fully integrated with business processes. Given the great variety of tools and standards inside industrial production environments, the IIRA specification deliberately presents a high-level description of the entities involved, proposing common architecture patterns fitting all industrial sectors. The specification strongly stresses the concept of *convergence of the IT and OT layers* at various points, underlining that the latter needs to be considered a common and required practice for enabling the transition to the new industrial automation. Viewpoints are the core layers of the IIRA model architecture, each of them conventions framing the description and analysis of specific system concerns. The Viewpoints of this reference architecture are depicted in Fig. 6.

The *Business Viewpoint* is focused on the values and objectives of business departments and stakeholders, such as the expected return of investment, the costs concerning the maintenance, and the product liability. The *Usage Viewpoint* relates to the operational aspect of using an IIoT system. The usage viewpoint is about concerns of entities external to a system. In this operational context, the user is defined as an entity that intentionally interacts with an IoT system (can either

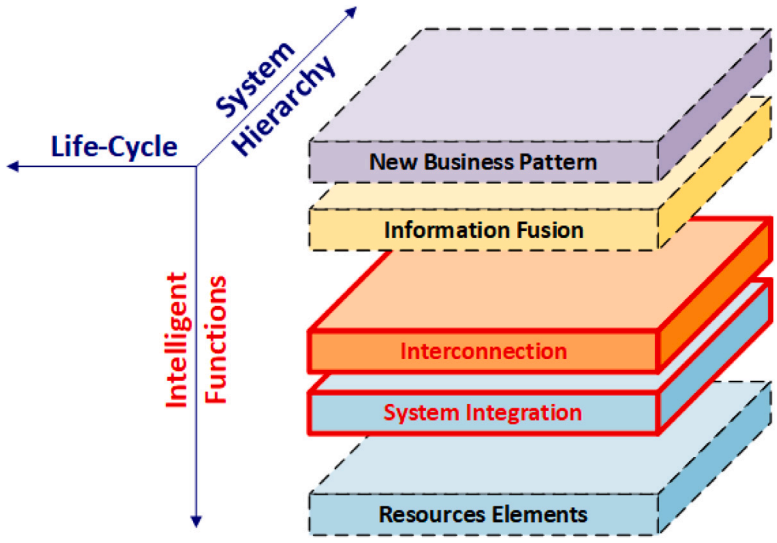

Fig. 5. IT/OT convergence in IMSA architecture.

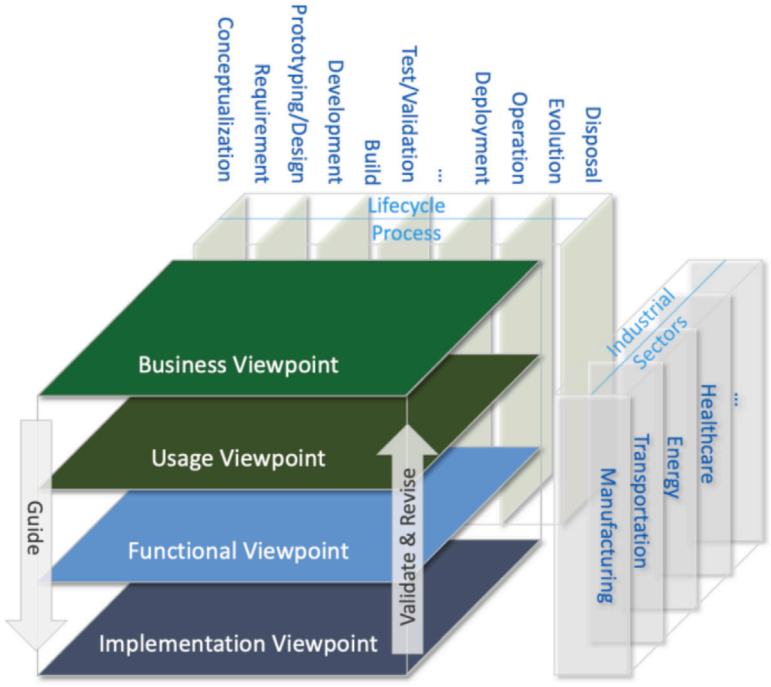

Fig. 6. IIRA viewpoints.

be a human or a digital system). The *Functional Viewpoint* addresses the concerns related to the functional capabilities and structure of an IIoT system and its components. This is a starting point for conceptualizing a concrete functional architecture. Among the proposed industrial internet viewpoints, the Functional is the one that mostly addresses the IT/OT integration of the layers in production plants. In Fig. 7, we depicted the functional domains included in the *Functional Viewpoint* of the IIRA architecture (Business, Information, Operations, Application and Control) and highlighted the functions that mainly contribute to the IT/OT convergence (red boxes). The Functional Viewpoint fosters a large use of IT both in business department and in the production control. Similarly to the RAMI model, IIRA recognizes asset digitization and communication as two paramount aspects of the transformation. It also stresses issues arising with the transformation, which mainly concern systems safety and resilience.

Finally, we remark that all the mentioned standardization initiatives have cybersecurity as a central and cross-cutting concern for the implementation of the I4.0 transition.

5. Related work and motivation

The maturity of the I4.0 vision has favored the spread of studies, research, surveys, and roadmaps addressing various aspects of the new industrial revolution and focusing on the technologies that are speeding up SMEs' transition to digital (Bittighofer et al., 2018; Trotta and Garengo, 2019; Abraham et al., 2016; Lu, 2017). After a thorough

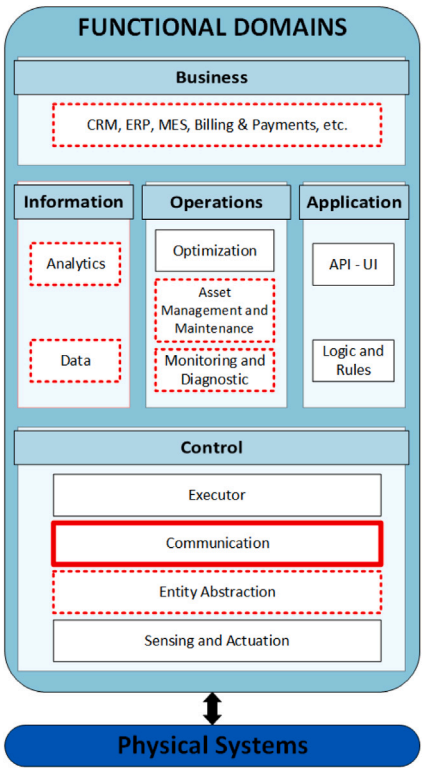

Fig. 7. IIIRA structure layers.

exploration of the body of literature in the field, we discovered that no survey explicitly assigns the IT/OT integration a pivotal role in the industrial digital transition. Yet, we found many research efforts that either touch on the integration topic or implicitly deal with its related implications.

In this section, we review the collected surveys in the aim of highlighting their contribution to the object of investigation and identifying important aspects not being covered instead. We make use of an evaluation grid to better define the extent to which each survey covers the IT/OT integration subject. With respect to prior surveys, ours proposes a complete, multi-dimensional analysis of the integration topic and performs a comprehensive systematic review of the literature in the field.

The surveys comparison grid depicted in the Table 1 builds upon the following analysis dimensions: (i) *Enabling technologies*: this refers to the presence in the survey of a thorough discussion of the technologies that are expected to produce an impact on the integration process; (ii) *Standardization activities*: this point refers to the presence of a review of past and ongoing standardization activities that are expected to support the integration; (iii) *Taxonomy*: this dimension accounts for the proposition of a taxonomy that frames the integration topics in a structured way and, accordingly, categorizes the literature works; (iv) *Covered topic*: this dimension accounts for specific integration area(s) covered by surveys. Regarding the latter point, we propose to consider the super-categories that populate the first layer of our taxonomy, which are *Communication*, *IT-driven support for OT*, *Advanced Industrial Control*, *Cybersecurity* and *Human Centricity* respectively. In our opinion, those categories are general and broad enough to make an exhaustive coverage of the integration knowledge domain. The reader will find more insights on the taxonomy design in Section 6.

Communication and networking are two relevant research areas that can provide a strong contribution to the integration of IT/OT layers. In that regard, the majority of literature proposals focus on either field machinery communication or modern *IT-oriented* communication protocols . According to authors of Ahmadi et al. (2018), wireless protocols and sensor networks are fundamental within CPS management and communication. They provide an overview of wireless connections based on classic network metrics such as reliability, throughput, and latency. The work analyzes the requirements of most CPS deployed in production plants and considers common IT wireless protocols such as Zigbee, Bluetooth, Wi-Fi, LoRaWAN, Passive Optical Networks (PONs), and Mobile Cellular Networks. From the literature analysis, the wireless communication technologies that meet the requirements imposed by converging CPS systems are PON and 5G, because they possess network features that fulfill CPS requirements. A communication-centric view of the integration is presented as well in Li et al. (2017), where authors also provide a novel architectural perspective of the industrial internet in modern factories. According to this work, the novel industrial architecture shall include a "cross-layer" concept, namely the cybersecurity, and 5 layers: connection, conversion, cyber, cognition, and configuration respectively. The layers implement a retroactive loop: the connection, conversion, and cyber layers gather data from work machines, the cognition layer elaborates such information and hands it over to the configuration layer, which retroactively commands the physical tier based on the taken decisions. Much attention is given to the connection layer, for which authors provide a thorough description and a comparison of many protocols like the Fieldbus CAN, Profibus, WirelessHART and CC-Link. Long range wireless technologies such as 5G, NB-IoT, and LoRa are also discussed in the paper as enablers of the IT/OT integration. This survey emphasizes the "everything-connected" concept fostered by many standardization bodies as one of the pillars of future production facilities.

In Aceto et al. (2019), authors explicitly point out that in the integration between OT and ICT a prominent role is played by the networked assets and by the employment of recently developed IP protocols and IoT applied to the industry. In the first part of the work, the authors list in chronological order the government initiatives promoting the digital transition, without providing though a deep analysis of each specific initiative's contribution. They identify many terms strictly related to the Industry 4.0 transition, such as smart manufacturing, smart factory, CPPS, and Industrial Internet. The work continues with the description of ten Industry 4.0 enabling technologies. Then, they describe various communication standards such as TSN, 6LoWPAN, CoAP, and MQTT, which contribute to transforming the current concept of production site into the modern one pushed by industry 4.0.

The integration of IT and OT layers may raise the level of context awareness within the production environment. Such a knowledge increases with the volume of operational data collected from OT and provides the companies with a complete view of their assets status as well as of the production processes in place. Many research communities are exploring the multifaceted adoption of Big Data in contemporary industrial settings, focusing on data-centric management, Big Data-driven production supervision, and data lifecycles in smart factories (Raptis et al., 2019; Qi and Tao, 2018; Tao et al., 2018). Data-centric management techniques, derived from extensive Big Data analyses, are integral in transitioning to Industry 4.0, notably impacting industries like oil and gas, healthcare, automotive, and marine. They act as catalysts for smart maintenance, prognostics, anomaly detection, and task scheduling (Raptis et al., 2019). Other research delves into Big Data techniques in production line management, emphasizing the contribution that Digital Twin techniques can bring to implement novel Big Data analysis patterns, which eventually pushes industrial production to a *Manufacturing-as-a-Service* model that supports products throughout their lifecycle (Qi and Tao, 2018). Here, data lifecycle management serves as a crucial foundational engine. Despite the acknowledged importance of these methodologies, companies recognize non-trivial challenges in widespread Big Data adoption, including the lack of clear standardizing communication protocols ad of uniform data formats, and call for ensuring network reliability of the factory-to-cloud path (Tao et al., 2018).

Table 1
Literature surveys addressing IT/OT convergence: a comparison table.

	Standardization initiatives	Enabling technologies	Taxonomy	Covered topic				
				Communication	Adv. industrial control	Data management	Security	Digital twin
Ahmadi et al. (2018)				•			•	
Li et al. (2017)				•	•		•	
Aceto et al. (2019)	•		•	•			•	•
Raptis et al. (2019)						•	•	•
Qi and Tao (2018)						•		
Tao et al. (2018)						•	•	
Oztemel and Gursev (2018)						•	•	•
Moghaddam et al. (2018)	•					•	•	•
Wortmann et al. (2017)						•		•
Lu (2017)					•			
Hofer (2018)		•			•		•	
Jbair et al. (2018)					•	•	•	•
Xu et al. (2018)					•		•	
Arica and Powell (2017)			•		•		•	
Lu and Weng (2018)		•	•		•			
Ebrahimi et al. (2018)			•		•			
Figueroa-Lorenzo et al. (2020)					•		•	
Gawanmeh and Alomari (2018)					•		•	
Alcaraz and Lopez (2022)						•	•	•
Bhamare et al. (2020)						•	•	
Conti et al. (2021)				•	•	•	•	•
Alves et al. (2023)								•
Adel (2022)							•	•
Xu et al. (2021)								•
Mourtzis et al. (2022)		•					•	•
Nahavandi (2019)		•						•
Our survey	•	•	•	•	•	•	•	•

The industrial landscape is renowned for its diversity, making it imperative to establish a unified IT/OT integration paradigm. This calls for the development of high-level architectures and the implementation of standards, guidelines, and prototypes within manufacturing environments. A pivotal initial step is defining goals that address critical facets of Industry 4.0, including standardization, resource management, and security (Oztemel and Gursev, 2018). The study in Moghaddam et al. (2018) puts the focus on the integration concept by elucidating the Industry 4.0 *Component*. This approach aligns with the guidelines outlined in the RAMI4.0 standard and draws a comparison with the IIRA model. Authors mention IBM 4.0 and NIST Service-Oriented architectures as exemplars of successful smart manufacturing implementations characterized by autonomous and self-contained services.

Model-Based System Engineering (MBSE) emerges as a pivotal methodology in the Industry 4.0 transition, facilitating the integration of IT and OT layers through the establishment of an integration tier connecting automation systems and stakeholders' processes (Wortmann et al., 2017). This study meticulously categorizes around two hundreds contributions based on the primary Industry 4.0 concerns addressed through MBSE tools. This categorization combines considerations and techniques utilized for describing the application domain, including various versions of UML, OWL ontologies, systems, and domain-specific modeling languages.

Another branch of the integration-related research addresses the domain of industrial control systems. Specifically, novel CPS architectures interacting with modern IIoT assets are proposed to improve the performance of control systems already in place like the SCADA and the DCS. In Hofer (2018), authors have collected studies that focus on the adoption of alternative CPS architectures to implement the servitization demanded by modern factories. Most of the analyzed works advocate that interconnecting CPS/IoT with ICT services is the key to achieve significant improvements of the product's life-cycle.

Some have reviewed literature works that pursue the adoption of cloud paradigms such as PaaS and IaaS to put IT computation capabilities at the service of OT processes (Jbair et al., 2018). Others focus on the seamless integration of physical industrial resources and IT processes to bring efficiency and raise profit of modern production plants. Again, IIoT is appointed to be the key to integration that modern industries need to use to make their production plants more efficient (Xu et al., 2018). MES systems too can play a crucial role in IT/OT integration but, unfortunately, there is no such a generic MES that fits every industrial use case. In the literature, many have proposed methodologies to guide the choice of proper MES and ERP tools with the support of a well-organized taxonomy (Arica and Powell, 2017).

Speaking of taxonomy, some literature works propose conceptual frameworks that aim to help the reader gain a comprehensive view of the industrial digital transition and, more specifically, of the IT/OT integration.

Authors of Lu and Weng (2018) delve into the semantic alignment of "Industry 4.0" and "smart manufacturing" terms. This work proposes a comprehensive examination encompassing market dynamics, as well as an assessment of the progress in key technologies, presented through a correlation matrix. In the proposed analytical framework, 19 pivotal technologies have been discerned, each intricately associated with the layers comprising the architecture of smart manufacturing, namely: sensor, integration, intelligence, and response tiers. Ebrahimi et al. (2018) addresses vertical and horizontal integration within production plants. This strategic approach facilitates predictive methodologies, paving the way for eventual self-organization and self-optimization of resources. The analysis delves into a specific use case within the automotive industry, outlining a domain for crafting a roadmap that guides automotive companies through the transition to Industry 4.0. In summary, the authors advocate that successful Industry 4.0 adoption necessitates automotive companies to prioritize the integration of IT and OT domains, emphasizing the integration of respective company departments.

On of the most interest-drawing branch of IT/OT integration, especially from the companies point of view, is Information Security. The integration of IT/OT layers bring new risks for equipment integrity and information confidentiality. The growth of the IACS attack surface requires the revision of existing security protocols and the development of new mechanisms that allow a secure and resistant connection between IT and OT in order to implement remote monitoring and actuation. Most works propose to enhance security of IIoT

and CPS systems deployed in manufacturing sites by targeting the vulnerabilities of communication protocols employed to exchange data between IIoT assets and monitor/control software (Figueroa-Lorenzo et al., 2020; Gawanmeh and Alomari, 2018). Within the proposed Vulnerability Analysis Framework (VAF), a methodology is offered to analyze potential eavesdropping of sensible data in CPS scenarios, which is considered the most frequent and dangerous breach in manufacturing environments. This kind of breaches could lead to the forgery of commands and configurations that remote control platforms send to the production sites with uncountable damages to the production lines and the company. The security threats to which the Digital Twins are exposed are of paramount importance when they need to be deployed in industrial environments. The aspect attracting the research attention the most is the interactions between the digital model and its physical counterpart. A taxonomy defining the security threats on this topic aims to increase companies awareness and to take adequate countermeasure (Alcaraz and Lopez, 2022). Speaking of industrial cybersecurity, two more research directions are worth mentioning. One focuses on using machine learning techniques for identifying deviations from normal system operations, particularly in control and process levels. The other involves categorizing ICS architectures, testbeds, datasets, and interconnections of distributed protocols with the purpose of understanding attack and defense mechanisms related to IT/OT integration. Overall, the consensus is that IDS emerges as the most effective strategy for safeguarding ICS against cybersecurity threats (Bhamare et al., 2020; Conti et al., 2021).

In the transformative landscapes of Industry 4.0 and the evolving Industry 5.0, characterized by the rapid integration of digital and physical systems, the concept of human-centricity emerges as a guiding principle to ensure that technological advancements prioritize the needs, experiences, and capabilities of individuals within the industrial ecosystem (Alves et al., 2023). In this context, human-centricity encompasses a multifaceted approach that spans user experience design, training and skill development, collaborative decision-making, safety and well-being, and change management (Adel, 2022). At its core, human-centricity recognizes that successful integration of IT and OT systems relies not only on technological prowess but also on the empowerment, engagement, and support of human operators and stakeholders (Xu et al., 2021). In the symbiotic collaboration between humans and machines promoted by Industry 5.0, human-centricity assumes even greater importance (Mourtzis et al., 2022; Nahavandi, 2019). In this regard, IT/OT integration aims to empower human operators to work alongside advanced technologies, leveraging their creativity, intuition, and expertise to drive innovation and problem-solving.

5.1. Filling the gap

Notwithstanding the indisputable research value of the explored surveys, which have been of great inspiration to our study, we believe that the state of the art is still missing a comprehensive systematic review of the integration topic.

Some relevant works (Aceto et al., 2019; Oztemel and Gursev, 2018; Lu, 2017; Lu and Weng, 2018) address many key aspects concerning the I4.0 transition, but in doing so they tend to be dispersive. While they deal with concepts and issues of *smart interconnected factories*, they fail to provide a clear taxonomy that frames such concepts. Because of the broadness and complexity of the industrial landscape, we argue that vertical approaches focusing on specific aspects are more effective in handling the challenging problems posed by the digitization process in industrial production environments. Although our approach touches on all enabling technologies of the digital transition, it digs more into IT/OT integration aspects. We also provide an orderly taxonomy that provides researchers and professionals with a technological path toward factory digitization, taking into account all fundamental aspects of this transition.

Many works deal just with issues of IIoT communication protocols, disregarding fundamental functional aspects such as management, processing, and storing of the data (Hofer, 2018; Xu et al., 2018; Ahmadi et al., 2018; Li et al., 2017). Ahmadi et al. (2018) presents an overview of wireless technologies used in manufacturing environments, whereas our survey adopts a broader perspective by considering all the major I4.0 enablers. Li et al. (2017) and Aceto et al. (2019) report on the state of the art of the industrial internet and communication technologies for I4.0, but do not present a well-defined taxonomy of the references and technologies involved in the transition process.

Some have proposed surveys on specific industrial control aspects such as MES (Arica and Powell, 2017), MBSE (Wortmann et al., 2017) or DT (Qi and Tao, 2018), while others discuss of technological enablers and reference models, omitting to touch on protocols, requirements, and strategies adopted at the lowest layers, thus providing only a partial perspective of the integration (Moghaddam et al., 2018; Moufaddal et al., 2019). Most of mentioned works address just the first layer of our taxonomy; we propose a deeper and more structured analysis of all integration concepts at all different architectural layers. Authors of Oztemel and Gursev (2018) and Moghaddam et al. (2018) propose a comprehensive analysis of the standardization initiatives and the related principles put forward, but they do not consider the impact of their adoption in manufacturing settings where the IT/OT integration is taking place. In Raptis et al. (2019) and Tao et al. (2018), authors address data processing issues but ignore important aspects like data ingestion and security, which are paramount in IT/OT integration.

Figueroa-Lorenzo et al. (2020), Gawanmeh and Alomari (2018) and Bhamare et al. (2020) focus on cybersecurity aspects. Some of them deal with the security of communication protocols (Figueroa-Lorenzo et al., 2020), while others (Bhamare et al., 2020; Conti et al., 2021) focus exclusively on safety, targeting industrial testbeds and machine learning techniques respectively. Being security a crucial aspect in industrial environments, we claim it must be addressed across all the building layers. In our work, we collected notable contributions discussing cybersecurity implications in the implementation of IT/OT integration, thus considering security as a *cross-layer feature*.

Finally, Lu and Weng (2018) and Ebrahimi et al. (2018) report on the benefits of IT/OT integration in specific business sectors, while Jbair et al. (2018) invokes the integration to solve individual use cases. Our survey does not focus on vertical application areas,rather, it aims to depict a global picture of all the benefits of IT/OT integration at both IT and OT levels.

6. IT/OT convergence: a comprehensive conceptual framework

We present a novel conceptual framework that depicts the state of the art of the IT/OT convergence topic in a systematic way. The framework grounds on a realm-oriented taxonomy that walks the reader through the convergence issues, threats, and opportunities under the perspective of technologies and paradigms that characterize IT and OT domains. We designed and proposed this novel framework to offer a fresh perspective on IT/OT integration and industrial digitalization. Our formulation builds upon the traditional layered architectures defined in established industrial standards (as discussed in Section 4). These standards typically adopt a rigid stack-oriented view, where each layer is presented as clearly separated and functionally isolated. However, this hierarchical representation does not adequately capture the reality of modern industrial ecosystems, where digitalization is ubiquitous and the integration of technologies, processes, and actors is increasingly pervasive. To overcome this limitation, we introduce the novel concept of realms. Unlike layers, realms are conceived as coexisting at the same level, inherently multi-connected, and mutually influencing each other. This perspective more faithfully reflects the cross-domain interactions that characterize IT/OT integration in practice. We propose a framework (Fig. 8) in which ***Communication*** and ***IT-Driven support to OT*** realms emerge as central pillars that

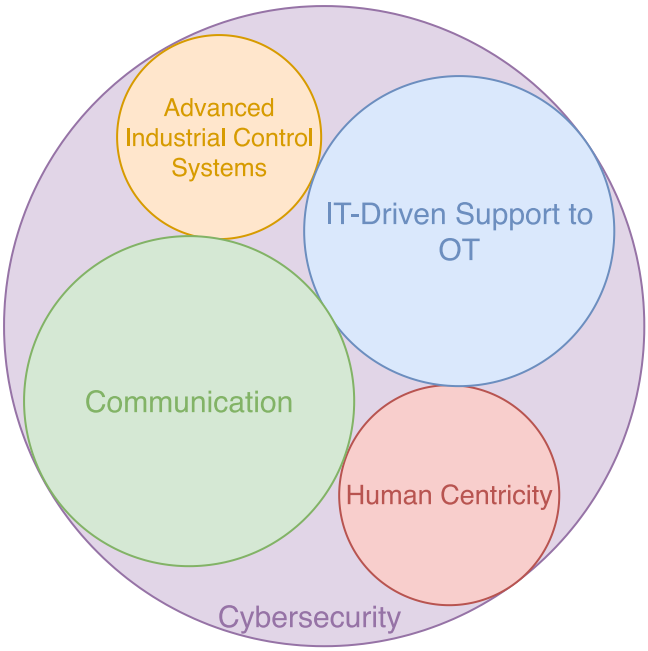

Fig. 8. IT/OT integration realms: the taxonomy's root concepts.

interact extensively with all other realms, including ***Human Centricity*** and ***Advanced Industrial Control Systems*** domains. At the same time, ***Cybersecurity*** is not confined to a single domain but rather acts as a transversal dimension, influencing, and being influenced by, all the others. This realm-oriented vision is directly validated by our survey of the state of the art: works nominally framed within one area (Human Centricity, or Advanced Industrial Control Systems) often leverage concepts, methods, or technologies from other areas, thereby underscoring the need for a more flexible conceptual framework. Moreover, transversal topics such as artificial intelligence, communications, and cybersecurity naturally manifest across multiple realms. For instance, AI-driven solutions for process optimization not only rely on communication infrastructures and IT applications but also influence human–machine interaction and PLC operations. Similarly, cybersecurity cannot be confined to a single domain: ensuring resilience requires coordinated measures that span networks, applications, devices, and human practices. By explicitly modeling these overlaps and interdependencies with ***tangent realms***, the realm-oriented framework complements and extends existing industrial models. It provides a more integrative conceptual foundation that captures both the structural dimensions inherited from standards and the pervasive cross-cutting challenges, such as AI and cybersecurity, that define real-world IT/OT integration.

The realm-oriented perspective introduced in Fig. 8 provides only the first level of the taxonomy, which will be further developed and enriched in Sections 8, 7, 9, 11 and 10 with relevant studies found in the literature. Each of the mentioned sections concludes with a brief analysis of the works reviewed under the specific theme addressed. For a more in-depth and comprehensive discussion of the survey's overall findings, readers are directed to Section 12. The figure depicting all taxonomy roots, branches and concepts can be found in Appendix A. The proposed taxonomy is strongly inspired by the research directions outlined by the most authoritative industry standardization movements. The three-axis vision provided by RAMI 4.0 and the layered viewpoints of the IIRA model guided us in the definition of a multi-tiered taxonomy. Following those standards approach, we make a clear separation between physical-related concepts characterizing shop-floor environments and higher-level concepts strictly pertaining to the office floor. Similarly to the Functional viewpoint of the IIRA model and the Communication layer in the Layers axis of RAMI 4.0 standard, we provide for an intermediate tier encompassing concepts representing communication-related aspects. Finally, taking again inspiration from the multi-dimensional view of IIRA and RAMI 4.0 standards, we define the cybersecurity realm as a whole-englobing realm since it represents all the security aspects which are trasversal to all other realms of IT/OT integration in the modern industrial scenarios.

The proposed taxonomy consists of four main root concepts, namely Communication, IT-Driven support to OT, Advanced Industrial Control Systems, Human Centricity, and an additional one that cross-cuts each of the above, i.e. Cybersecurity. In their turn, all concepts are further broken down into finer categories so that a hierarchical structure is eventually proposed.

The survey revealed that the **Communication** realm plays a key and dominant role in IT/OT convergence. For that reason, we intentionally address it first (see Section 7). The Communication realm includes works that focus on the development of increasingly configurable, performing, and robust communication networks. This taxonomy emphasizes the central function of secure and reliable network communication to encourage the spread of approaches that facilitate IT/OT convergence within production sites. The implementation of these characteristics in the networks of the IT domain is transferred to the production plants that undertake the transition to Industry 4.0, contributing to the advancement of industrial communication protocols in the OT domain. As depicted in Fig. 9, it comprises *Northbound* and *Southbound* categories. The communication-related taxonomy not only contains the works linked to the modern networking protocols that over the last few years have contributed to the spread of IIoT devices that are of enormous support to IT/OT convergence, but it also comprises the latest innovations in the field of network solutions employed in sectors that have critical applications, which must comply with very strict requirements and respond in real-time. The *Northbound* category describes solutions based on the use of IIoT hardware, the IoT protocols themselves, and the use of modern software-based networks in the industrial field. The latter *Southbound* category comprises approaches working at the lowest levels of communication, e.g., innovative wired and wireless protocols for both deterministic and non-deterministic purposes. The **IT-Driven support to OT** realm deals with technologies that address data management in converging environments (see Section 8). As shown in Fig. 10, the realm is further decomposed into the *Processing strategies* category, encompassing all data management solutions like, e.g., those AI-based or the ones leveraging semantics, and the *Provisioning models* category, that encompasses architectural solutions exploiting modern computing paradigms to build convergent systems.

The **Advanced Industrial Control Systems** realm encloses all literature contributions approaching the transition to the convergent world through innovative proposals for the management and control of production plants and industrial assets (see Section 9). This category, illustrated in Fig. 11, includes complex systems like *Distributed Control* and *Software-defined Control*. These classes embrace all contributions that pursue the IT/OT convergence objective by proposing enhancements of components already employed in production sites such as *Architectures* Systems and *On Premise* industrial controllers (e.g., softwarized PLCs).

The **Human Centricity** realm includes literature contributions that focus on the novel aspect of IT/OT convergence, where humans are seen as a key element of the factories of the future (see Section 11). In this context, the integration and collaboration between humans and machines represent the true added value for this new concept of industry. The taxonomy, depicted in Fig. 13, encompasses new industrial *frameworks*, addresses modern work approaches for advanced industry scenarios (i.e., *Lean Production and Sustainable Manufacturing*), and proposes the innovative concept of *Society 5.0*. Finally, Human Centricity includes the most tangible example of Human–Machine integration, i.e., the *Collaborative Manufacturing*.

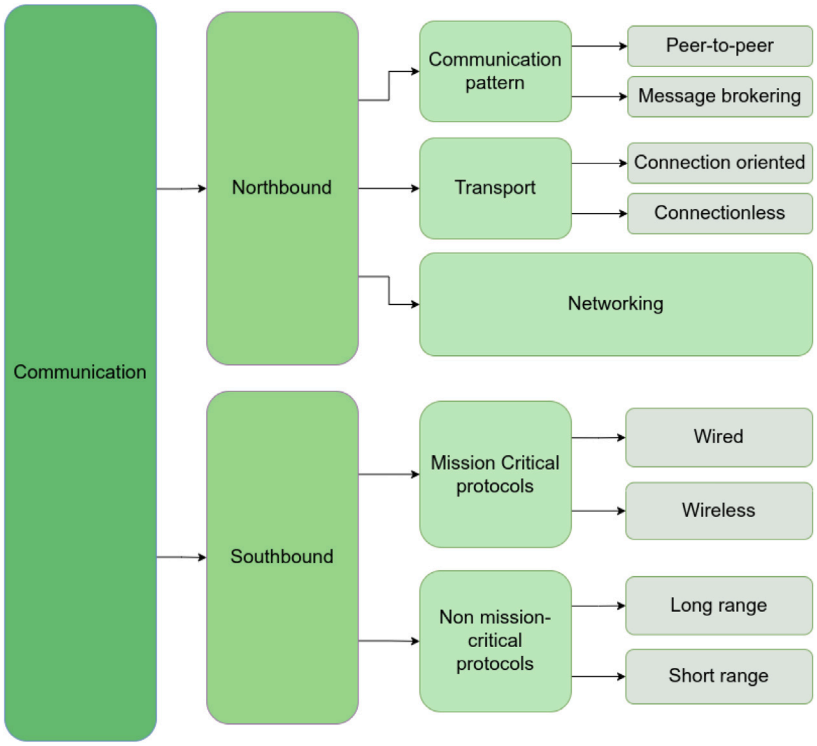

Fig. 9. Communication taxonomy.

The vast majority of the surveyed works, independently of the category they belong to, argue that cybersecurity is an urgent matter that converging IT/OT systems must face with. To his end, we envisioned a **Cybersecurity** realm cross-cutting all taxonomy realms (see Section 10). Specifically, considering the typical hierarchical structure of company departments, at the lowest layers it is imperative to protect M2M communication and ensure the safe functioning of work machines so as to minimize the risk of harm to both people and the surrounding environment, as well as leakage of information. At the highest layers, where the data is gathered from both OT and IT departments, a correct management of information needs to be enforced along with a clear identification of the rights of actors/stakeholders to access sensitive data. In Section 10, the ordering adopted to present the taxonomies (Communication, IT-Driven support to OT and Advanced Industrial Control Systems) will be retained to describe the cybersecurity topics, i.e., firstly the Communication-related concepts, secondly those concerning the IT-Driven support to OT and finally those pertaining the Advanced Industrial Control Systems.

7. Communication taxonomy

Communication is crucial in IT/OT integration, as it facilitates the bi-directional data flows between managerial and operational departments. A significant portion of the literature reviewed in this survey falls under this category, indicating that communication is a primary concern of research communities that focus on IT/OT integration. We distinguish between works addressing higher-level aspects of communication, such as transport protocols and networking, and those dealing with field connectivity.

The Communication taxonomy is depicted in Fig. 9. The Northbound branch encompasses several protocols and data pathways facilitating the communication from the lower tiers to the higher tiers of industrial system architectures. This branch addresses modern industrial settings and include all the proposals that aim to bridge industrial edge nodes (OT level) with factory in-sight servers or cloud systems, whether they are private or public. On the other hand, the Southbound branch includes protocols enabling communication *in-the-field*. Such connectivity facilitates the transmission of data, commands, signals from central systems to individual machines, sensors, or controllers on the factory floor, supporting the coordination and control of industrial processes. Literature dealing with field protocols falls in this category. In both branches, we initially introduce key concepts, then further categorize each branch into more fine-grained classes, and ultimately delve into relevant studies within each class.

7.1. Northbound

In order to address the relevant concepts of the Northbound branch, we resort to a layered approach that recalls the ISO/OSI stack. We break down the Northbound branch in three categories where, communication-wise, the IT/OT integration is addressed at application, transport and networking level respectively. Top-down, the resulting taxonomy break-down will further include the *Interaction* branch, collecting proposals that target both plain client–server (C/S) interaction and IIoT message-based protocols, the *Transport* branch, comprising literature that addresses innovative ways of dealing with data transport, and the *Networking* branch, which basically gathers proposals addressing the virtual networking topic.

7.1.1. Communication pattern

Communication protocols play a significant role in Industry 4.0, serving as key components in the integration of OT and IT. In this taxonomy branch, we break down the research efforts addressing innovative interaction approaches in the peer-to-peer (P2P) and the message-brokered categories, respectively. The former envisage direct and *synchronous* interactions between the communicating parties (to which many refer to as the "client–server" way), while the latter basically prescribe *asynchronous*, event-based interactions mediated by third-party broker (which is also known as the "publish–subscribe" approach).

Synchronous communication is at the base of most IT distributed systems where smaller software units (components) communicates with

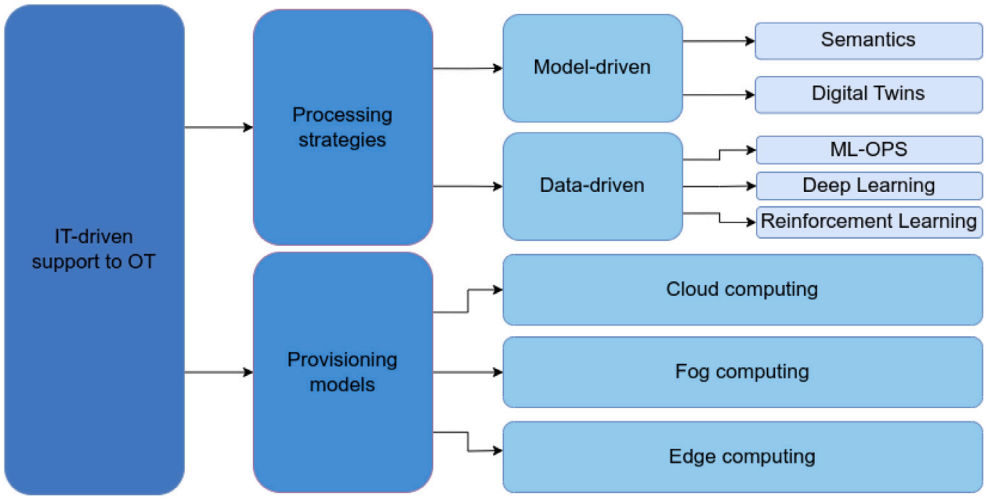

Fig. 10. IT-Driven support to OT taxonomy.

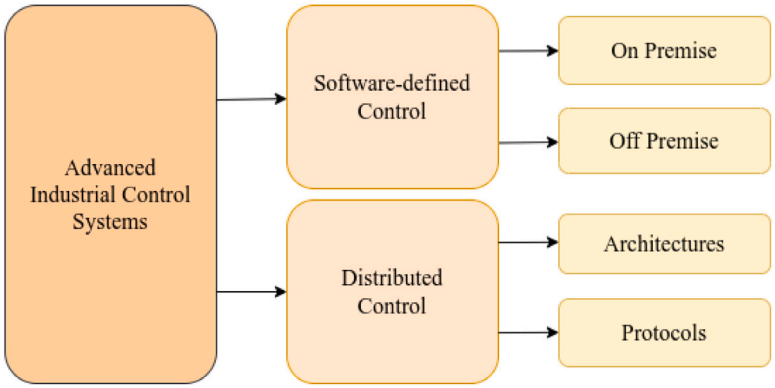

Fig. 11. Advanced Industrial Control Systems taxonomy.

each other according to a request–response pattern. Particularly, synchronous communication is commonly used in Service Oriented Architecture (SOA) (Group, 0000) implementations, with services that rely on higher-level communication protocols such as SOAP (Consortium, 0000) or the Representational State Transfer (REST) (Fielding, 2000). SOA has been adopted extensively in the last two decades as the architecture of choice for structuring distributed computing systems in general, including industrial systems (Zhang, 2019; Cândido et al., 2009; Morariu and Borangiu, 2012). The mentioned communication protocols supports the adoption of the SOA paradigm along the OT-IT path, as witnessed by the many efforts being reported in the literature (Siqueira and Davis, 2021). While SOAP has been the preferred choice of the first wave of SOA industrial solutions (Cagnin et al., 2018; Ferrer and Lastra, 2017), which featured the employment of service monoliths, with the advent of the micro-services architectural styles REST has emerged as lightweight protocol that perfectly fulfills the interaction needs of micro components in integrated industrial environments (Bigheti et al., 2019a; Mena et al., 2019).

Within the OPC UA architecture (OPC UA) (Unified architecture, 2019), a protocol was proposed for exchanging data both within the shop-floor (e.g., from PLC to HMI) and between the OT and IT departments. OPC UA operates using a client–server architecture, where servers are responsible for gathering and organizing data from various sources, and clients perform operations such as reading/writing data, subscribing to data updates, and invoking methods exposed by the server. The standard guarantees support for both P2P and publish–subscribe communication patterns. Also, OPC UA is communication protocol independent, as it provides mappings to several communication protocols like TCP/IP, UDP/IP, WebSockets, AMQP and MQTT.

Message-based protocols such as MQTT (Mqtt, 0000), CoAP (Coap home, 0000) and AMQP (Amqp home, 2008) have drawn the attention of industry for a twofold reason: they enforce a loose coupling between the operational and business layers and enhance the scalability of machinery in production settings. Adaptability, performance and compliance to standards are key features that have pushed practitioners to extensively adopt these IIoT protocols in the transition process to Industry 4.0 and 5.0. The TRIDENT framework, proposes a strategy to translate the variety of protocols into a common model (Benedick et al., 2019). The framework implements three main steps: the definition of a common model, the development of wrappers, and the creation of applications. The work defined two operation modes to test the last step of the methodology, an OPC UA application to test the client–server mode, while MQTT, the O-MI (Open Messaging Interface), and O-DF (Open Data Format) protocols to test message-oriented operations. Integration wise, a strong requirement is the need of message-based mechanisms that can effectively help ingesting and lively processing the big amount of data originating from the OT level. The framework developed in Bosi et al. (2020) proposes an open-source platform capable of interacting with shop-floor machines powered with IIoT protocols such as MQTT and AMQP. The tests demonstrate that, by virtue a microservices-based architecture and the use of message-oriented protocols, the framework can acquire data from the work machines in (near) real-time and offer selective access mechanisms

for various Industry 4.0 stakeholders. An illustrative example of integration in industrial environments can be found in the smart grid vertical, where the WiseGRID project (Stratogiannis and Gkiala-Fikari, 2018) seeks to connect smart grid components and IoT devices for monitoring and control purposes. The WiseGRID project aims to define business models and integration strategies for contemporary European smart grids. In this initiative, authors leverage the MQTT and AMQP protocols to enable the integration of both legacy assets and modern IT devices and software. Finally, Nguyen-Hoang and Vo-Tan (2019) proposes an original heterogeneous IoT gateway capable of providing interoperability between field buses (CAN, Modbus, RTU/TCP) and the modern protocol suite (e.g., MQTT, AMQP, and CoAP). The proposed gateway is built on top of Linux-based software like Docker and Node-Red and allows the fast deployment of containers that integrate the dialects of different protocols. Latency in reading/writing PLC registers is used as an indicator of the communication network performance, while measurements are carried out on a cloud-based platform.

7.1.2. Transport

In the context of IT/OT networking, researchers often explore the TCP/IP stack and associated standards, with the purpose of making innovative proposals at the transport layer. While most of efforts attempt to find innovative solutions that leverage *connection-oriented* and reliable type of communication channels, others have explored *connection-less* approaches (i.e., UDP-based) that strive to guarantee close-to-real-time performance.

The Multipath TCP (MPTCP) (Internet Engineering Task Force (IETF), 2024) specification proposes to modify the original TCP layer of the TCP/IP protocol suite to improve redundancy and network resiliency. TCP multipath as a message transport solution that can stimulate the development of advanced and distributed industrial applications whose software components can be deployed both in OT (i.e., close to machines in the field) and in IT settings (i.e., in relatively remote Fog or definitely remote Cloud). In this scenario, TCP multipath enhances the robustness and resiliency of TCP-based interactions between "distant" components. Unlike the original TCP protocol's single-path strategy, MPTCP employs a multi-path approach, allowing the transport connection to concurrently utilize multiple network paths. A notable work proposes the adoption of DQN to reach human-level intelligence in managing complex networks in scenarios where IT and OT layers converge. More in detail, a DQN agent is capable of analyzing and learning from network traffic and interacting with the MPTCP settings to adopt the best policy and derive the best route to send packets, augmenting the network efficiency and its performance (Pokhrel and Garg, 2021). Morawski and Ignaciuk (2021) argue that, despite the concurrent use of a few transmission channels offered by MPTCP enhances the quality of service and reliability of communication, scarce attention has been paid to the energy issues suffered by such approach especially in resource-constrained devices populating the IIoT domain. They developed a systematic tuning procedure for improving the energy efficiency of MPTCP data transfer, and thoroughfully tested it to show that it can help boost the overall MPTCP performance, both in terms of energy saving and throughput stability. In the literature, some works exist that leverage AI, and specifically DRL, to support reliable and fast data transfer over converging networks such as the WiFi and the 5G (Xu et al., 2019; Wu et al., 2020). Stemming from the consideration that all of those DRL-based approaches suffers from long (re)training time, authors of Pokhrel et al. (2021) propose the design of a novel distributed transfer learning (TL) framework to maximize MPTCP communication networking performance for the I4.0 environment. Experimental results prove that the proposed novel architecture is capable of instantly adapting to changing network constraints and dramatically evolving topology, which are typical of I4.0 integrated network scenarios.

QUIC is a transport protocol originally developed by Google (Langley et al., 2017) and recently standardized by the IETF (Iyengar and Thomson, 2021). In addition to addressing significant TCP limitations for the Industrial Internet of Things (IIoT), such as more precise packet acknowledgment and re-transmission, QUIC also provides additional benefits particularly relevant for industrial scenarios, as they contribute to lower latency while still ensuring reliable and secure communication. Authors of Fernández et al. (2021) analyze the performance of QUIC as a transport alternative for Internet of Things (IoT) services based on the Message Queuing Telemetry Protocol (MQTT). Experiments were carried on for a variety of wireless access networks, which included WiFi, cellular and satellite. To demonstrate the feasibility of MQTT-on-Quic in industrial scenarios, authors set-up an three-layered IIoT infrastructure scenario featuring communicating parties at the Things, Fog and Cloud levels respectively. Results obtained in terms of overall end-to-end delay under tough conditions (e.g., lossy channels, high frame error rate) were compared with that exhibited by the traditional TCP/TLS approach. The tests proved that QUIC clearly outperforms TCP, especially for connections with low RTT and high packet erasure rates. QUIC also yields a more predictable behavior, with much less variability in the results. Supported by these results, authors conclude that QUIC is an appropriate communication protocol to guarantee robust, secure, and low latency communications over IIoT scenarios.

7.1.3. Networking

As companies seek to implement the transition to the "all-connected factory" fostered by I4.0, SDN and NFV emerge as crucial enablers. The flexibility offered by both technologies creates an environment where IT and OT systems seamlessly coexist. SDN operates as the control plane in network management, overseeing infrastructure, running services, and delivery policies from a holistic perspective. Through directives to the SDN controller, dynamic adjustments to network parameters can be made, tailored to the specific needs of supporting applications. NFV replaces physical hardware for network functions with virtualized alternatives, offering flexibility in deployment. This allows entities like routers, load balancers, and firewalls to operate within virtual machines. The adoption of NFV allows organizations to achieve cost savings by deploying adaptable virtualized functions rather than investing in dedicated hardware. The advent of these technologies has opened the door to several research developments that investigate the profitability of harnessing them in the OT world. The main research directions target the employment of SDN and NFV paradigms to define new conceptual frameworks and innovative working models.

Software-Defined Cloud Manufacturing (SDCM) is a new concept derived from the combination of SDN and the Cloud-Based Design and Manufacturing (CBDM), a new model widespread with the new Industry 4.0 vision. In the SDCM architecture, there is a clear separation between hardware and software planes. The hardware layer is distributed and comprises physical assets, while the software plane consists of a virtual layer where business applications operate. Additionally, there is a control plane within the software layer that abstracts the complexity of underlying networks and protocols, providing a user-friendly interface for application developers operating in the virtual layer (Thames and Schaefer, 2016).

Digital IoT Fabric (Yannuzzi et al., 2017) is a framework that aims to brings IT capabilities near the industrial production plants. It exploits the powerful features of the ETSI's NFV MANO and the OpenFog architecture. The model proposed in this framework allows for the uniform management of *fabric* resources, regardless of whether the software is a control program running in the fog or cloud, or a network function. It effectively implements orchestration, monitoring, and network virtual functions to bridge the gap between IT and OT layers seamlessly.

The advancement of intelligent industrial environments through the integration of innovative features based on the SDN and NFV paradigms is a promising avenue for research. Specifically, features such as industrial traffic flow management, dynamic network and Service Level

Agreement reconfiguration through QoS adjustments, and the deployment of dynamic security policies are drawing considerable interest within the research community (Shrestha and Lin, 2020; Kupzog et al., 2020; Sadi et al., 2024).

7.2. Southbound

This section introduces the second portion of the Communication taxonomy, depicted in the bottom of Fig. 9. A common feature of most communication protocols, claimed by many literature works, is the integration of OT Fieldbus protocols with those that emerged and are widespread in the IT world. In this section, we provide an overview of both ultra-reliable *Mission Critical protocols* and robust *Wireless protocols* used in modern production facilities. Contextually, we report literature works in the field.

7.2.1. Mission-critical protocols

The TSN standard developed by the IEEE 802.1 working group (Time-Sensitive Networking (TSN), 2020) responds to the need of making the resources connected to the network aware of the timing, thus enabling precise synchronization among them.

TSN and the IEC/IEEE 60802 protocol (the TSN profile for Industrial Automation) enhance Ethernet communications by offering time synchronization, increased network reliability, efficient traffic shaping, and minimal latency. However, there are still concerns about adopting TSN due to the complexity of configuring it in large and dynamic network topologies and issues related to protocol security (Lo Bello and Steiner, 2019).

Despite the security concerns, TSN is largely considered a promising research direction in mission-critical communication protocols fields, especially when used alongside other popular field protocols such as OPC-UA, where time-constrained task are carried over TSN, while latency-tolerant ones can be run over other protocols. This helps to standardize the approach to industrial communication layers (Bruckner et al., 2019).

To tackle the complex matter of network devices' configuration, some works leverage Configuration Agents to continuously monitor the network status and to dynamically change network configuration whenever requested. Configuration Agents are meant to be deployed on smart switches or more in general on fog nodes. Among the others, two main works pursuing this direction are worth mentioning: the first proposes NETCONF protocol (developed by Internet Engineering Task Force (IETF)) as a standard modeling language to model managed objects, while the latter focus on allowing the user to define and manage different streaming polices though the introduction of a User Network Interface (Gutiérrez et al., 2017; Pop et al., 2018).

Making wireless communication protocols sensitive to time requirements is a crucial step toward achieving converging industrial scenarios. Recent research suggests that leveraging 5G technologies and mmWave communication offers a promising solution to address time sensitivity. Beyond wired Ethernet-based deployments, recent research has increasingly focused on the integration of TSN with 5G and emerging 6G networks, aiming to extend deterministic communication into mobile and flexible industrial environments. The combination of TSN and 5G enables Ultra-Reliable Low-Latency Communications (URLLC) services while preserving precise time synchronization and bounded latency. One line of work introduces a simulation framework that bridges TSN and 5G domains by addressing two critical aspects: synchronization across heterogeneous segments and QoS-aware flow mapping, showing how translator elements defined in 3GPP specifications can ensure deterministic performance in smart manufacturing scenarios (Da Silva et al., 2025; Agustí-Torra et al., 2025). Still, a new standardization effort is deemed necessary for industries to securely adopt wireless protocols for time-critical applications (Cavalcanti et al., 2019).

Time Slotted Channel Hopping (TSCH) is a medium access control (MAC) protocol standardized in the IEEE 802.15.4e amendment (Std, 2020; Teles Hermeto et al., 2017). It is designed to provide highly reliable, deterministic, and energy-efficient communication, making it well-suited for industrial applications and, in our opinion, one of the most promising wireless protocol in the modern converging scenarios. In TSCH, the communication is organized into discrete time slots, each long enough to accommodate the transmission of a data frame and its acknowledgment. These time slots are grouped into a repeating schedule, ensuring deterministic behavior. Devices communicate based on this schedule, which eliminates contention and ensures collision-free operation. To enhance reliability, TSCH employs channel hopping, where the communication channel used in each time slot is determined by a pseudo-random sequence. This mechanism mitigates the effects of interference and multipath fading, which are prevalent in industrial environments. TSCH serves as the foundation for higher-layer protocols like 6TiSCH, which integrates TSCH with IPv6, in the aim of enabling the adoption of IPv6 in industrial standards and boosting the convergence of OT networks with IT systems in modern industrial scenarios (Jin et al., 2016; Tabouche et al., 2023; Pettorali et al., 2024; Minet et al., 2017). In industrial automation, a trend involves establishing precise communication schedules between devices using protocols like WirelessHART and ISA 100.11a, fostering reliable connections in low-power networks. The 6TiSCH working group concentrates on implementing TSCH in industrial scenarios, integrating IPv6 over IEEE 802.15.4 to create secure and reliable networks since 2014 (IP, 0000).

The 6TiSCH provides the ultra-low-power consumption and high reliability features of TSCH to the upper layer of IPv6 stack, allowing the researcher to re-design the architectural stack of the protocols and showing how the advancements in some layers (e.g., the introduction of WirlessHART and ISA100.11a protocols) can support the accomplishment of the IT/OT integration (Dujovne et al., 2014).

The research community is exploring the adoption of 6TiSCH in industrial environments with particular focus on distributed scheduling approach employed in factory automation. One of the most notable approaches proposes a decentralized traffic-aware scheduling algorithm (DeTAS) deployed on an industrial open wireless sensor networks (OpenWSN). This protocol aims to fulfill some important convergence requirements, i.e.: (a) extremely low-latency from data production to data ingestion at the application level, (b) minimum medium usage, by alternating sending and receiving cells in TSCH protocol (Accettura et al., 2015).

7.2.2. Non mission-critical protocols

IEEE 802.11ax and IEEE 802.11ay are two protocols of the IEEE family that strive to mitigate the uncertainty of wireless connections, thus increasing the confidence of companies that intend to implement IT/OT convergence by adopting wireless connection-based protocols. The IEEE 802.11ay protocol (Standard, 2020b) proposes an enhancement of the IEEE 802.11ad WLAN specification, which defines wireless communication at 60 GHz. It operates at frequencies higher than the 802.11ax, therefore has a larger bandwidth but is less prone to overcome obstacles such as walls or architectural barriers. The IEEE 802.11ax (Standard, 2020a) (also known as Wi-Fi 6) aims to attain the determinism of wireless networks through the use of the multi-user version of OFDM technology to access the medium, i.e. the Orthogonal frequency-division multiple access (OFDMA).

The primary spectrum-based categories are unlicensed and licensed. The unlicensed spectrum includes new low-power wide-area (LPWA) protocols like Long Range (LoRa) and Sigfox, the Bluetooth standard and its variant Bluetooth Low Energy (BLE), and IEEE 802.15.4. The licensed spectrum encompasses all 2G, 3G, 4G, and 5G protocols for industrial communication. To evaluate these protocols and highlight their features and optimal use cases, in Liu et al. (2019) an appropriate framework is proposed. This framework enables network architects to consider all factors affecting network performance at each level of

Table 2
Contributions in the literature to 'Communication'. Symbols: • denotes substantial focus; ∘ indicates marginal discussion.

[#]	IT-Driven support to OT					Communication						Advanced ICSs				Cybersecurity	HC
	Processing strategies		Provisioning models			Northbound				Southbound		Software-defined Control		Distributed Control			
	Model-Driven	Data-Driven	Cloud	Fog	Edge	Comm.	Pat.	Transp	Net	MC	Non MC	Off Premise	On Premise	Architectures	Protocols		
Stratogiannis and Gkiala-Fikari (2018)	∘					•										∘	∘
Bosi et al. (2020)			∘			•		∘			∘				∘	∘	
Benedick et al. (2019)						•											
Nguyen-Hoang and Vo-Tan (2019)			∘			•		∘									
Pokhrel and Garg (2021)		∘				∘		•			∘						
Morawski and Ignaciuk (2021)								•	∘								∘
Xu et al. (2019)		∘						•	∘								
Wu et al. (2020)		∘						•		∘	∘						
Pokhrel et al. (2021)		∘						•	∘								
Langley et al. (2017)								•	∘								
Fernández et al. (2021)								•	∘		∘					∘	
Yannuzzi et al. (2017)			∘	∘	∘	∘			•			∘				∘	
Shrestha and Lin (2020)			∘		∘	∘			•		∘				∘	∘	
Kupzog et al. (2020)			∘		∘	∘			•			∘		∘			
Thames and Schaefer (2016)			∘			∘			•								
Lo Bello and Steiner (2019)						∘		∘		•	∘				∘		
Bruckner et al. (2019)			∘	∘		∘		∘		•	∘	∘		∘		∘	
Cavalcanti et al. (2019)						∘				•	∘						
Gutiérrez et al. (2017)						∘				•	∘						
Pop et al. (2018)			∘	∘		∘				•							
Vilajosana et al. (2020)						∘		∘		∘	•					∘	
Dujovne et al. (2014)						∘					•					∘	
Accettura et al. (2015)						∘					•						
Yi et al. (2017)			∘					∘			•			∘	∘	∘	
Liu et al. (2019)	∘		∘			∘			∘		•						
Amendola et al. (2017)						∘					•					∘	

industrial systems An example of framework is proposed to measure the performance of a Cloud-Based SCADA system that uses Modbus communication in various plant scenarios (Yi et al., 2017).

In addition to the discussed frameworks, research also focuses on deploying RFID sensor networks (RFID-SNs) in modern industrial networks within production plants. The study uses a real smart grid cabin on Favignana island (Italy) as a testbed for detecting anomalies in the electrical system, preventing unauthorized access, and managing complex events. The adaptability of the hierarchical RFID sensor system highlights its versatility in collecting and analyzing extensive statistical data for various industrial applications (Amendola et al., 2017).

7.3. Communication layer wrap-up

In Table 2, we propose a list of the surveyed works along with the specific taxonomical concepts addressed in the IT/OT convergence framework. Row-wise, the solid dot (•) identifies the main concept a work primarily focuses on, while hollow dots (∘) indicate concepts that are marginally touched. The same approach will be used in Sections 8.3 and 9.3, where synoptic tables are shown for literature contributions covering IT support to OT and advanced industrial control aspects respectively.

As the reader may notice, the protocols designed to support mission-critical and non mission-critical communication among IoT devices are extensively proposed in modern industrial networking scenarios. The strict requirements imposed by OT push for the development of deterministic network technologies. Among those, TSN seems to be the most promising one and is believed to smooth out the technological discrepancies between OT and IT. On the wireless front, 6TiSCH has emerged as a promising IP-capable protocol that promotes a substantial form of convergence.

On a higher level, message-brokering is gaining ground as the most suitable interaction model in the ecosystem of digital objects that populate the factory of the future. While its adoption in OT has been historically "confined" to data exchange among devices populating the shop-floor (e.g., through CoAP, MQTT), at IT level asynchronous messaging is more and more harnessed to implement invocation of service functions in microservice-powered applications. As proposed by some literature efforts, the asynchronous interaction way natively adopted in OT can be the key for extending the service computing to OT environments. Indeed, message-brokering promises to offer the right level of decoupling that irons out technology discrepancies of communicating peers. It is also worth noticing that many proposals indicate the cloud continuum provisioning model as an enabler of the convergence.

It is no surprise that, for the majority of works, cybersecurity is a huge concern in consideration of the potential cyberattacks that could threat the communication path between IT departments and shop-floor. This specific topic will be thoroughly addressed in Section 10. Finally, despite network virtualization techniques have become very popular in telco environments, SDN/NFV do not seem to have received the same attention in industrial settings. Our study has revealed that a more solid security framework could help boosting a wider adoption.

8. IT-Driven support to OT taxonomy

In modern industrial environments, production plants produce huge amounts of data. These volumes are mostly heterogeneous in both formats and data sources, thus requiring standardized procedures to process them and generate value for the companies. From those big, heterogeneous and apparently unrelated data, both OT and IT departments can gain high-level insights to make informed decisions and implement secure digitization of the plants.

In this section, we explore branches of the literature that propose methodologies, techniques, tools, and infrastructures commonly used in IT and ICT that, when applied to modern industrial OT, enable the integration, processing, and smart management of heterogeneous data and production processes, ultimately optimizing the factory production at a reduced cost. Fig. 10 depicts the expanded tree of the *IT-Driven support to OT* root concept. On the one hand, we surveyed the literature works that have borrowed data representation and processing techniques from IT to propose innovative approaches aiming to improve the performance of industrial processes at OT level. On the other one, we sought for proposals that stress the opportunity of adopting innovative IT computing models and infrastructures to further support OT digitization.

8.1. Processing strategies

The upper branch of the IT-Driven support to OT sub-tree collects works mostly addressing data processing techniques. Processing strategies can be conveniently split in two major branches:Model-Driven, which comprises proposals privileging approaches requiring the full knowledge of the domain and the dynamics of targeted systems, and Data-Driven, collecting efforts that build up the domain knowledge by exploiting the variety and volume of data collected from the field.

8.1.1. Model-Driven

Industrial automation is pervaded by model-centric processes where automated decisions are driven by heterogeneous data produced by a great variety of sources. In regards to technology interoperability, both departments and stakeholders have shown great interest in exploiting semantic technologies and ontology-driven solutions to improve interdepartmental and inter-enterprise collaborations (Lin and Harding, 2007; Sampath Kumar et al., 2019). In industrial contexts, besides the OWL Web Ontology Language-based solutions (Schevers and Drogemuller, 2005), the Common Information Model (CIM) conceived by the Electric Power Research Institute (EPRI) seems to be a good and flexible candidate language to build common power system models on which electric sector operators and device and plant designers can work together (Britton and deVos, 2005; Khare et al., 2011). The electric field is a very fruitful ground for the research on data semantics and ontologies, indeed, smart grid and power production facilities are drawing the interest of the community. In this field, the need emerged of adopting common data models on which to build a convergent architecture that bridges IT and OT layers. The WiseGRID project is a European initiative targeting the definition of a business model and of a data model for modern European smart grids. Its goal was to design a harmonized model among all the entities through the identification of all data flows inside the production plant. To iron out the data heterogeneity, a model with common entities was adopted, such as those taken from the Open Automated Demand Response (OpenADR), which provided non-proprietary interfaces to interconnect Distributed Energy Resources (DER) management software and control devices. In this context, it was proposed the employment of the Universal Smart Energy Framework (USEF) to enhance the flexibility of the data model and the common language Device Language Message Specification/Companion Specification for Energy Metering (DLMS/COSEM) to define the rules for data exchange among IT and OT company departments (Stratogiannis and Gkiala-Fikari, 2018). Similar approaches have been followed in two national initiatives targeting electric grids and power production plants, in Turkey and in Slovenia respectively (Doğdu et al., 2014; Souvent et al., 2019). In the first one, the crucial role of modern Decision Support Systems (DSS) for the technological progress of smart grids was explored, asserting that these systems not only produce economic benefits for end-users, but also enhance understanding of the relationship between consumers and the Distribution Service Operator (DSO). More in detail, this work investigates the standards that model the information space, IEC 61850 and IEC 61970, then it focuses on the integration of business tools such as Geographic Information Systems (GIS), Automated Meter Reading (AMR), and Outage Management Systems (OMS), that turn electric grids in actual smart ones. The secind work focuses on the use of CIM-based architecture for integrating the IT/OT layers in power production facilities in Slovenia. The main purpose of the standards belonging to the CIM family, namely IEC61970, IEC61968, and IEC62325, is to unify tools and information at IT and OT levels under a common schema, thus building a shared service-based architecture for data exchange. This work proposes an integration platform that includes an Integration bus, CIM repository, Interfaces to integrated systems, and an Implementation process. The CIM repository centrally stores unique identifiers and network topology, while the interfaces integrate existing systems such as GIS, Distribution Management Systems (DMS), and Meter Data Management System (MDMS). This approach reduces the risk of multiple specific integrations, preventing the undesirable "spaghetti architecture" side effect in IT/OT integration.

Modeling resources through semantic techniques and ontology-based approaches is a valuable way to achieve integration also from other perspectives. Semantic techniques can be used for abstracting away network complexity and decouple W3C Web of Things (WoT) existing applications from the networking layer in TSN-based environments (Sciullo et al., 2020). This work fosters the management of QoS at the application level and the semantic configuration of TSN networks, which would bring the same advantages of the CUC/CNC TSN mechanism in the management of communication by defining a series of URI schemas to cover the use cases of the OPC UA communication and the NETCONF configuration protocol. In this specific case, new terms are introduced within the W3C specifications, WoT Architecture and WoT Thing Description (TD), facilitating smart management of enterprise networks. Devices, portrayed as semantic "Things", need to advertise their capabilities by being annotated with a Quality of Service (QoS) attribute. This enables applications following the WoT approach to understand operation requirements and reserve communication streams accordingly. On the same page, another relevant research work proposes a Ontology-based Resource Management Framework (ORMF) as a way to achieve integration. This framework provides a unifying ontology for IoT systems and the Software-Defined Data Centers (SDDC) (data centers providing resources, networking storage, computation, and orchestrating multi-cloud and multi-site infrastructures), that allows a common dialect on resource management and allocation in IT/OT convergent environments. The proposed unified ontology results from the integration of different ontologies, such as the OpenIoT Ontology, the Semantic Sensor Network (SSN) ontology, and the Cloud Computing Ontology (CoCoOn). This framework aims to deliver several benefits for IT/OT convergence, including improved overall security through the application of IT policies to OT environments and streamlined device onboarding using a unified ontology. This approach ensures consistent device descriptions across both IT and OT layers. Moreover, adopting an ontological approach eliminates the need to develop interfaces and bridges from scratch to connect IT and OT systems (Koorapati et al., 2018).

The digital twin paradigm has gained prominence as organizations seek to bridge the IT/OT gap (Bokhtiar Al Zami et al., 2025; Ren et al., 2025). While it is possible to encounter many Digital Twins (DTs) definitions declined into diverse industrial research fields (Grieves and Vickers, 2017; Grieves, 2011; Grieves and Vickers, 2016), the research community agree that DTs are virtualized computerized counterparts of physical systems that continuously exchange data to stay as much synchronized as possible and keep the digital model adherent to reality (Negri et al., 2017; Khan and Ahmad, 2025). From the implementation point of view, a DT may be of one of the following types: *physical-model* DT, which is a type of digital twin powered by physics-based models (i.e., derived from physical laws and expressed in terms of mathematical equations) to simulate the behavior and performance of a physical asset or system; *data-driven* DT, which depends primarily on historical data and relies on machine learning to derive a system model (Chen et al., 2025). While we are aware of this dual implementative approach, since most of the literature works follow the first one in our taxonomy, we opted for collocating the DT concept under the Model-driven category.

In industrial scenarios, DT-based systems are used to monitor production line/machine health (or more generally for managing the complex product lifecycle) by mirroring the behavior of both physical industrial assets and processes (Fantozzi et al., 2025). To properly simulate the production process, DTs face a well-known issue of industrial environments, i.e., data sharing across diverse departments. DT systems have to overcome lack of standardization, implementation costs, interaction with employees, and the strict industrial regulations (Singh et al., 2018; Editorial, 2020). DTs can also be utilized to improve factory efficiency and enhance the resilience and security of production lines and machinery. They achieve this by offering a safe and secure platform for integrating IT and OT systems. These systems provide accurate models and simulations of the factory, either from a specific or holistic perspective, enabling the analysis of cyber-attacks, behavioral deviations, and unexpected production scenarios. This capability supports the development of the "Factory of the Future" (Dietz and Pernul, 2020; Bécue et al., 2020).

As mentioned earlier, DTs can be the virtual replica of several entities inside the industrial environments. This concept perfectly fulfills

the needs of predictive maintenance applications. Being a replica of the real production environments, the digital model can be used to monitor the behavior of OT assets and enforce proactive corrective actions to preserve or prolong the machine health (Akira Kanazawa, 2019). In Borghesi et al. (2021), DTs are implemented as distributed components deployed over a continuum of resources spanning factory-owned Edge machines and the Cloud. In the Cloud, authors leverage AI/ML techniques to train predictive maintenance models with historical data gathered from the shop floor. Trained models are then shifted to the Edge where they are fed with fresh sensed data. The connection between the physical assets and their digital counterpart is guaranteed by a data pipe that originates from the field sensors, crosses the Edge, and terminates in the Cloud.

8.1.2. Data-Driven

The lower branch of the IT-Driven support to OT sub-tree addresses all those works focusing Data-Driven approaches. Under this hat, many techniques have been proposed that try to equip machines with human-intelligence capabilities. ML is a subset of AI techniques that, by means of supervised and unsupervised learning approaches (such as the Reinforcement Learning (RL)), can easily transfer knowledge to the machine and update it without having to redesign the system. In production sites, multi-layered Artificial Neural Networks (ANN), trained with advanced techniques such as Deep Learning (DL), Federated Learning and Deep Reinforcement Learning (DRL), are employed to track IIoT devices and react to anomalous events as humans would do (Chen et al., 2019; Yang et al., 2020; Niu et al., 2025).

Across a variety of applications, data-driven approaches in Industry 4.0 and 5.0 focus primarily on enhancing efficiency, enabling dynamic reconfiguration of components or systems, and monitoring and controlling products and production processes. In complex industrial scenarios, such as oil and gas (O&G) or automotive sectors, AI and its techniques, like Machine Learning (ML), play a crucial role. These methods analyze current data flows in the context of historical data to generate predictive insights. These insights contribute to improve system efficiency and enable a more effective management of industrial IIoT assets (Stracener et al., 2019; Colombi et al., 2024; Keller, 2019).

Machine learning techniques like Deep Learning (DL) and Reinforcement Learning (RL) are being increasingly applied to this field, driving advancements in areas such as predictive maintenance, quality control, process optimization, anomaly detection, and autonomous control (Gahlawat et al., 2023; Hicham et al., 2023; Nian et al., 2020; Kegyes et al., 2021). DL is a powerful technique for anomaly detection in industrial settings. Advanced neural network architectures have been designed to effectively identify deviations from normal operating conditions or product specifications. This approach has garnered significant attention and adoption in both research and industry, leading to promising solutions that enhance the accuracy and efficiency of anomaly detection systems across various industrial sectors (Sajitha et al., 2024; Ameri et al., 2024). DL-based reconfiguration is a topic which is largely getting adopted in industry especially when the reconfiguration targets the industrial networks. DL technique can be applied to provide support services and reconfiguration to that industrial networks in a very mobile and dynamic scenario such as Non-Terrestrial Networks (NTN) in mines, disaster recovery, and/or crisis management sites. For example, DL techniques applied to NTN can assist space-borne and airborne platforms in adapting their characteristics to potential interferences, attenuations, and fading, due to wireless long-range connections (Michailidis et al., 2020). RL and Deep Reinforcement Learning (DRL) are widely adopted in the advanced industrial scenarios to enhance decision-making, process control and cyber-security and privacy at OT level. RL turns out to be particularly effective for decision-making and process control activities, where these algorithms are capable to learn from the specific environment, operational conditions, or even ever-changing requirements for optimizing the decision-making process or the whole production phases (Deng et al., 2022; Liu et al., 2021). Another application of DRL algorithms in industry focuses on detecting intrusions or malicious attacks. These techniques can dynamically reconfigure or adapt security policies to prevent smart device hijacking and neutralize attackers. A practical example of applying DRL is its use in DQN-based algorithm to identify the optimal attack transition policy used to hijack the IT/OT devices in smart grid environments. This technique managed to equalize the performance of graph-search approaches, without having to physically observe the system under attack (Liu et al., 2020).

MLOps is a new paradigm that enables the fast development, reconfiguration and deployment of industrial, microservice-based applications in predictive manufacturing, predictive maintenance, and smart monitoring scenarios (Bachinger et al., 2024). MLOps is a very promising research topic that includes challenging open issues like the management of ML models between cloud and industrial edge, and the hoe to integrate ML models and their continuous deployment with industrial processes and applications (Bustamante et al., 2023; Faubel et al., 2024). A more tangible example is given in (Venanzi et al., 2023a), where MLOps is used to measure the drift of industrial process or product parameters and trigger the re-deployment of new ML model, microservices' configurations, or appliances settings configuration to adjust the running industrial process.

8.2. Provisioning models

Compute provisioning models such as the Cloud, Fog and Edge create a convenient and flexible environment where traditional OTs and modern ITs can converge to provide enhanced efficiency, productivity, and smart decision-making. The Cloud has become an appealing model to industry for its capabilities of accommodating in a prompt and flexible way several industrial workloads, such as near-to-real-time monitoring of machines, collecting and centralizing vast amount of data sensed from the field, running off-line and on-line analytics such big data (Al Jawarneh et al., 2025). On the other end, Fog and Edge computing in the industrial context promise to extends cloud computing capabilities to the edge of the network, closer to the devices and systems that generate data, thus enabling real-time processing, reduced latency, and improved security for critical industrial applications.

In our taxonomy, the category representing such models is depicted in the bottom end of Fig. 10. The literature proposes solutions (frameworks, middlewares, etc.) that take advantage of the benefits offered by the mentioned provisioning models, both individually and in a combined fashion that practitioners usually refer to as *Cloud Continuum* or *Compute Continuum*. The Cloud Continuum enables organizations to dynamically place workloads and data across distributed infrastructure, from centralized cloud data centers to on-premises systems and edge devices, based on factors like latency, cost, compliance, and performance needs. This approach provides flexibility, scalability, and interoperability to support diverse and evolving business and technological requirements. In the following, we report a synthetic description of some representative works in the field.

8.2.1. Cloud Computing

Modern I4.0 realities need a flexible and cost-effective approach to the manufacturing process, due to the shorter product cycles and time-to-market schedules, as well as competition with global partners. Employees, customers, and supply chain players demand continuous and remote connections to business activity, in order to have a more informed and controlled knowledge base on which to build precise decision-making engines. Cloud computing, with its private, public, or mixed arrangements, is capable of giving this kind of connections and flexibility and it has been the preferred solution in the last years for the manufacturing sector, enough to be labeled with the term Cloud Manufacturing (Li and JÖrn, 2013; Tao et al., 2014). The even stricter requirements in terms of performance, high information

availability, security, and confidentiality have favored "in-home" deployment solutions, such as those based on the employment of edge computing resources within the production sites to support the work machines flexibly (Chen et al., 2018; Li et al., 2019; Qi and Tao, 2019). The Service Oriented Architecture (SOA) paradigm has spread in the industrial sector to help IT departments to develop and maintain services that support production and business processes. SOA is often applied to manufacturing (Lilan et al., 2007). Employing service-oriented platforms in manufacturing improves flexibility in terms of the coexistence of different kinds of services, IoT assets, and interoperability among machines and nodes from different vendors and support for different protocols (Cândido et al., 2009; Venanzi et al., 2021, 2020). The combination of the SOA paradigm with a continuous integration and developments (CI/CD) techniques puts the basis for a plug-and-play IT architecture capable of meeting the market demand because of its high degree of flexibility (García-Domínguez et al., 2013; Morariu and Borangiu, 2012). The employment of Cloud Computing paradigm in industry leads the research community to think about platforms for bringing cloud services into industrial plants. The platforms, addressing the servitization of the production plants, can provide cross-organizational services that can be offered to many stakeholders in the I4.0 value chain. Numerous global initiatives, including Industrie 4.0, EFFRA, and the RAMI 4.0 framework, aim to advance platforms for industrial plant management. Notable IoT platforms, like Microsoft IoT Azure and AWS IoT Core, offer pre-packaged services, particularly in machine learning. Additionally, digital manufacturing platforms provide diverse data management services. The emergence of these platforms highlights the necessity for programmatically integrating IT and OT levels, offering a centralized approach for companies to manage equipment and information in corporate production environments (Gerrikagoitia et al., 2019; Tazzioli et al., 2023; Venanzi et al., 2023b).

In addition to global initiatives that promotes Cloud platform for industries, several research projects aims to design and develop cloud continuum frameworks to facilitate the transition towards I4.0/5.0. ArrowHead, ArrowHead Tools, and Disrupt are just three of the large plethora of the European projects targeting the IT/OT integration. From these projects, many valuable outputs emerged that were eventually deployed in real industrial scenarios. DISRUPT focuses on facilitating the transition to I4.0 through a data drive system that supports real-time decisions in response to disruptive events such as the failure of a production line or a delay in the raw materials provisioning. It focuses on designing a reference architecture facilitating IT/OT convergence, addressing decision-making and task scheduling in manufacturing. This proposed architecture supports real-time analysis, vertical/horizontal integration, and stakeholder involvement in product lifecycle management. Comprising five layers, Physical, Virtualization, Operational, Decision, and Visualization, it converges various technologies in the industrial environment. The architecture manages assets, aggregates data, homogenizes information, processes data through manufacturing knowledge modeling, and displays insights to end-users based on access policies (Kavakli et al., 2018). Arrowhead, and Arrowhead Tools are two European projects that promote the adoption of a microservice SOA-based framework to build, implement and deploy Automation and digitalization solutions in European industrial scenarios by enhancing component integration, standardization, and interoperability between industrial plant assets and IT services. This framework has found a wide adoption by many relevant industrial scenarios into partners' factories. More in details, Eclipse Arrowhead Framework has been used for critical IIoT applications within I4.0 contexts which deployments typically present interoperability, management, and third-party device integration issues, requiring human intervention along the engineering process of the systems (Montori et al., 2023, 2021). As it emerged in even in Arrowhead context, interoperability inside CPS systems is considered the key enabler of IT/OT convergence. This interoperability is often provided by employing the SOA approach to tackle the heterogeneity of communication between IT and OT layers, and it drives to an higher level decoupling between the products and the production lines, which then put the basis for the production of new products with no changes made to the control production tools (Zhang, 2019).

8.2.2. Fog computing

Many industrial innovation projects and research directions are targeting the adoption of fog computing paradigm for achieving the IT/OT convergence in modern I4.0/5.0 scenarios. Digital IoT Fabric is a converged platform for bridging the IT/OT gap inspired by the ETSI NFV MANO and OpenFog reference architectures. The Digital IoT Fabric platform can orchestrate applications at the edge and cloud sides, by spanning multiple fog nodes at the plant level in order to bring IT capabilities to the OT environment. The employment of fog computing and NFV aim to overcome the heterogeneity given by the proliferation of proprietary protocols and hardware and improve the management of highly distributed resources with limited computational powers (Yannuzzi et al., 2017).

Another fog computing platform, inspired by the European initiative Fog Computing for Robotics and Industrial Automation (FORA), aims to provide deterministic communications, and smart resource management to industrial environments. The architecture's fog nodes run in both IT and OT domain applications and are connected to each other, to sensors/actuators, and to the cloud. The fog architecture is capable of mediating the divergences between IT and OT application requirements by leveraging on the protocols interoperability (such as OPC UA, MQTT, CoAP), fast resource provisioning, and network determinism (i.e., TSN) (Pop et al., 2021).

TSN is a core communication technology for fog architectures, especially if they are deployed on nodes distributed into OT and IT domains. A relevant research proposes a fog-based architecture in which computational and storage capabilities are integrated into fog nodes connecting to each other by way of a deterministic TSN connection. The proposed fog architecture has two key features: replacing ProfiNet/RT with TSN for a reliable cloud connection, and implementing slicing techniques for running different applications on shared resources in spatial–temporal isolation (Barzegaran et al., 2020).

Meeting deadlines is crucial in industrial settings. If, on the one hand, TSN to pursue this goal in terms of communication, on the other one additional efforts are required to take care of scheduling aspects and process priority policies. These aspects are paramount for providing acceptable Quality of Control for industrial time-critical and non-critical applications. To this end, a research study proposes a simulated annealing-based metaheuristic to schedule the tasks in the most suitable fog node and use an Earliest Deadline First (EDF) scheduling policy tested in different fog deployments. This approach identifies the fulfillment of all timing requirements, both time-critical and non time-critical (Barzegaran et al., 2019).

8.2.3. Edge Computing

Edge Computing has seen significant adoption in industrial scenarios to address the high bandwidth and low latency demands of modern smart industrial applications. It has emerged as a key enabler for IT/OT convergence in industrial environments. A primary advantage of Edge Computing is its ability to drastically reduce latency, which is critical for time-sensitive decision-making processes and enhancing communication. It introduces determinism in IT/OT convergence scenarios, ensuring reliable and predictable communication flows essential for industrial operations. Thing-edge-cloud Collaborative Computing Decision-making (TCCD) is a method that employs edge computing as interconnection technology between OT and IT layers to meet customized time production needs and for providing real-time data collection, computation resources, and storage directly at manufacturing sites. TCCD aims to improve delivery deadline meetings by adapting and customizing the production to customer's orders through

Table 3
Literature contributions to 'IT-Driven support to OT'. Symbols: • denotes substantial focus; ∘ indicates marginal discussion.

[#]	IT-Driven support to OT					Communication						Advanced ICSs				Cybersecurity	HC
	Processing strategies		Provisioning models			Northbound			Southbound			Software-defined Control		Distributed Control			
	Model-Driven	Data-Driven	Cloud	Fog	Edge	Comm. Pat.	Transp	Net	MC	Non MC		Off Premise	On Premise	Architectures	Protocols		
Koorapati et al. (2018)	•		∘	∘	∘			∘						∘		∘	
Doğdu et al. (2014)	•													∘			
Sciullo et al. (2020)	•					∘			∘					∘	∘		
Souvent et al. (2019)	•													∘	∘		
Dietz and Pernul (2020)	•											∘				∘	
Akira Kanazawa (2019)	•											∘					
Singh et al. (2018)	•											∘					∘
Editorial (2020)	•	∘										∘					
Bécue et al. (2020)	•	∘	∘			∘						∘					∘
Borghesi et al. (2021)	•	∘	∘		∘					∘		∘					
Stracener et al. (2019)		•	∘			∘											
Keller (2019)		•	∘														
Bustamante et al. (2023)		•	∘		∘												
Faubel et al. (2024)		•															∘
Venanzi et al. (2023a)		•		∘	∘												∘
Sajitha et al. (2024)		•															
Ameri et al. (2024)		•															
Michailidis et al. (2020)		•	∘	∘	∘	∘		∘		∘				∘		∘	
Deng et al. (2022)		•								∘							
Liu et al. (2021)		•							∘								
Liu et al. (2020)		•												∘		∘	
Gerrikagoitia et al. (2019)			•			∘								∘			
Kavakli et al. (2018)			•														
Montori et al. (2023)			•		∘												∘
Montori et al. (2021)			•														
Jiang and Wan (2021)			•		∘		∘			∘							
Barzegaran et al. (2020)	∘	∘	∘	•					∘					∘	∘	∘	
Pop et al. (2021)	∘		∘	•	∘				∘					∘	∘		
Barzegaran et al. (2019)			∘	•			∘										
Tazzioli et al. (2024)			∘		•			∘	∘								
Bellavista et al. (2024b)		∘	∘		•			∘	∘								
Bellavista et al. (2024a)			∘		•			∘	∘								
Badar et al. (2019)					•				∘			∘		∘			

an highly dynamic supply chain. Edge computing has a pivotal role in TCCD being the enabler that allows to overcome the uncertainty of the production systems (Jiang and Wan, 2021).

Edge computing enables real-time data processing and provides very low latency at the very edge of the network. These features are essential in Industry 4.0/5.0 environments since they enable the migration of the services by-need and with a drastically reduction of downtime. Stateful services are becoming increasingly important in Industry 4.0, their adoption spans from decision-making applications up to anomaly detection and predictive maintenance. Supporting the stateful service migration in modern industrial environment enabled by the adoption of edge computing paradigm is a challenging research direction. Some relevant works addressed this topic by proposing a modification of the core of Kubernetes, a world-wide recognized, open-source microservices orchestrator, to efficiently migrate stateful services in modern industrial environment targeting the minimization of the service downtime and the service continuity (Bellavista et al., 2024b,a; Tazzioli et al., 2024).

Edge computing is used in a smart industrial scenario to also overcome the uncertainty of I4.0/5.0 networks. Huawei and Festo provide tools to enableedge architecture for deterministic communications. The edge environment is enriched with deterministic IP routers that emulate the co-existence in the I4.0 scenarios of many flows with different policies, priority, deadlines, and requirements typical of vPLC applications. This kind of deployment, based on edge computing to provide deterministic communications, allows us to provide very bounded latency and jitter values to vPLC scenarios by allocating the routes and the bandwidth for the different flows mixed in the same network (Badar et al., 2019).

8.3. IT-Driven support to OT layer wrap-up

We provide some synthetic considerations on the literary works that have tackled IT/OT convergence from the IT layer perspective. Surveyed contributions are reported in Table 3. The study revealed that, while model-driven techniques are basically adopted with the purpose of supporting the industrial control, more and more researchers explore strategies driven by the Big Industrial Data to extract insights useful to improve the performance of industrial processes under multiple aspects. Most of DT-based solutions for the IT/OT convergence purpose focus on software simulations of the industrial processes and assets. Some build data-driven DTs that leverage AI to enforce the control and optimization of industrial production. ML/DL approaches are embraced to process, validate and extract knowledge from raw data for the purpose of automating IIoT-driven processes. On the other side, Cloud/Edge and modern service-oriented paradigms promise more agile and versatile management of the production plants. The surveyed works pursue the IT/OT convergence goal by proposing multi-level architectures that envision a remote cloud layer to offload heavy computation and data aggregation that cannot be handled on the company premises. Finally, the edge layer enables the management of services and applications with strict requirements. Often, the Edge is where a tight integration between IT and OT takes place.

9. Advanced Industrial Control Systems taxonomy

In Section 3, we discussed the role of ICSs in driving the industrial production automation and remarked that such systems are expected to evolve with the advent of I4.0. In this section, inspired by the proposals found in the recent literature, we illustrate a conceptual framework that captures the advancements made in the industrial control field that contribute to a concrete integration of IT and OT.

The devised taxonomy on Advanced ICS is depicted in Fig. 11. After a careful analysis of surveyed literature, we identified two main trends which reflect the research interest over the industrial control topic: the study of more flexible way of implementing the control functions and the study of enhanced industrial control architectures that cope with the distributed nature of control components in complex CPSs. On the one hand, the advent of more robust and flexible software frameworks and tools has encouraged researchers to propose the adoption of "softwarized" control components to replace or complement traditional control hardware. In this context, we found numerous efforts discussing the potential of implementing softwarized control functions both within and beyond the shop floor. (better known as *remote control*). On the other hand, following the latest evolution in SCADA systems, several lines of research are exploring advanced and distributed control architectures, which call for greater openness in OT and effective IT/OT interoperability.

9.1. Software-defined Control

The upper part of Fig. 11 depicts the branch of the taxonomy that collects research works proposing the softwarization of industrial

control components. Due to their high re-programmability, PLCs are the core components of the industrial automation that lend themselves to softwarization. By the term Virtual Programmable Logic Controller (VPLC), practitioners refer to a software-based version of a traditional hardware PLC that is capable of running on general-purpose computing platforms such as PCs, servers, or virtual machines. In I4.0 scenarios, the adoption of VPLC brings considerable benefits such as, to name a few, ease of system reconfigurability, scalability to control system growth, remotization of control functions, and tighter and better integration with IT systems. In the following, we report literature works suggesting the adoption of VPLC and advocating their deployment both within and outside of the factory premises.

9.1.1. On Premise

Notwithstanding the mentioned benefits, there are some critical OT-level challenges that need to be overcome for the VPLC to be considered a viable and reliable solution. One of them is the need to preserve determinism, i.e., the ability to control and keep communication latency and jitters as low as possible. In that regard, a critical aspect is choice of a suitable software virtualization technique that can guarantee a low impact on the VPLC performance in terms of reaction time. The Virtual Machine approach could turn out to be excessively onerous for real-time environments. Some tried to overcome the virtualization limits by working on hypervisors. More in detail, the research focuses on real-time hypervisors for running VPLC instances. The proposed architecture is a convergent system in which PLCs' real I/O is separated from the control logic, which is managed by the VPLC entities, while the connection and the routing are entrusted to an SDN-enabled Ethernet network deployed within the plant (Cruz et al., 2016). The performance of the system proved acceptable, but the need for further investigation on still stays on. Under this perspective, a valuable work proposed new deterministic IP networks (IETF Deterministic Networking (DetNet) working group) to guarantee real-time industrial Ethernet (RTE) communications at the OT level. The work aimed to prove the goodness of the protocol in a mixed traffic scenario on a single deterministic IP network by incorporating the sensitive VPLC I/O traffic with general-purpose traffic (i.e. connecting IP cameras) to the routers (Badar et al., 2019).

To better comply with OT real-time constraints, researchers have started looking into more lightweight virtualization techniques such as the containerization. In Tasci et al. (2018), the proposed project modularizes real-time control applications and relies on a hardware abstraction layer to improve portability (separating domain logic from the platform or hardware-specific code) and flexibility. The authors show the ability of their middleware to cope with the real-time constraints of typical industrial environments thanks to the employment of Linux machines with specific kernel configurations. In addition to virtualized PLC control functions, data acquisition procedures are also important to keep the latency low (Bigheti et al., 2019b). Data Acquisition service (DAQ) transparently offers higher-level applications a data acquisition service that uses underlying hardware modules allocated in the process, while a softwarized PLC (SoftPLC) is responsible of controlling I/Os. As a result, applications do not need to comply with I/O hardware specifications or with the code (software) necessary for obtaining the required variables. Finally, SoftPLC, based on the OpenPLC project, combines the features of a PLC with the benefits of an open hardware and software architecture (openplc, 0000).

9.1.2. Off Premise

Being VPLC a servitization of physical PLC functions, it can potentially be deployed anywhere, even outside of the production premises. In the literature, some have explored the opportunity of implementing remote control by way of VPLCs deployed on remote cloud resources. A VPLC deployed in the cloud will suffer all the inherent well-known disadvantages of the cloud approach, which in shop floor control context can result to be even more impactful. Unscheduled disconnections along with the non-real-time communication path of cloud deployments is probably the biggest issue that undermines the feasibility of remote VPLC. To face this issue, in the literature two directions have been proposed: (i) an hybrid mechanism that switches to local control (e.g., in a local cloud/edge) when remote access to the virtual control is denied; (ii) a PLC-as-a-service implementation that exploits a real-time hypervisor to mitigate the latency which is mainly due to poor resource-sharing mechanisms (Gilani et al., 2016; Givehchi et al., 2014). Both these approaches have been successfully tested in two real industrial deployments. Nevertheless, from the tests it emerged that VPLC are unfit to serve hard real-time scenarios.

9.2. Distributed Control

SCADA systems have evolved through three different generations (Cai et al., 2008; Ujvarosi, 2016). The first generation of SCADA (1960–1970) was mainly characterized by monolithic deployments. In the second SCADA generation (also called "distributed", 1970–1990), the introduced novelty was the possibility of decentralizing the control function. Finally, in the third generation (so called "networked" SCADA) industrial systems have been re-shaped into the actual networked remote systems. In there, the main improvement is the adoption of open system architectures enabling access to SCADA functionalities across a WAN, rather than just inside the plant's LAN, thus enhancing the flexibility, reliability and robustness of the control also in case of disasters. Vendors produce RTUs/PLCs with ethernet connectivity and the employment of COTS components in the system makes it easier for the customers to add third-party peripheral devices, such as monitors, hard drives, and printers. SCADA systems also take advantage of the advent of well-known IT standards, such as the IEC 61131-3 (IEC, 0000), which delivers specifications concerning the control programming languages.

Similarly to SCADA, Distributed Control Systems (DCS) are computerized control systems used for automated process control. DCS are designed to control complex, large-scale processes within a single facility or plant. In DCS many control loops are implemented, in which autonomous controllers are distributed throughout the system, but there is no central operator supervisory control. SCADA and DCSs have very similar objectives and implementation strategies. While SCADA systems are more prone to data gathering and supervision, DCSs work best in terms of real-time control and operation (Zawra et al., 2019; Šindelář and Novák, 2012; Lobur et al., 2011; Pariyani et al., 2016). As evidenced in the remainder of this section, the depicted evolution has contributed to a slow but progressive opening of the shop floor to the IT world.

The Distributed Control taxonomy is depicted in the bottom of Fig. 11. This class includes both open and interoperable control architectures and protocols that are expected to support IT/OT interoperation.

9.2.1. Architectures

Among the innovative approaches that have tackled the grid modernization journey, the Advanced Distribution Management Systems (ADMS) stand out as aggregate infrastructures encompassing multiple sub-systems such as Distributed SCADA (DSCADA) system, OMS, GIS, and DMS (Cochenour et al., 2014; Agalgaonkar et al., 2016). Due to their integration capabilities, these systems are being deeply investigated in modern industry 4.0 (Jamei et al., 2016; Hozdić et al., 2020; Meliopoulos et al., 2013).

In this context, the integration of ADMS/SCADA systems represents a step further towards the transition to a smart grid deployment. The ICT technological advancement and in the spread of ADMSs the factors that made the integration of the IT and OT layers possible, and the development of architectures providing this type of integration allows to overcome the many issues that might occur in the IT/OT convergence implementation in smart grid and smart industrial plants (Ahmed and Roy, 2016; Lim et al., 2016).

Table 4
Literature contributions to 'Advanced Industrial Control Systems'. Symbols: • denotes substantial focus; ∘ indicates marginal discussion.

[#]	IT-Driven support to OT					Communication					Advanced ICSs				Cybersecurity	HC
	Processing strategies		Provisioning models			Northbound			Southbound		Software-defined Control		Distributed Control			
	Model-Driven	Data-Driven	Cloud	Fog	Edge	Comm. Pat.	Transp	Net	MC	Non MC	Off Premise	On Premise	Architectures	Protocols		
Badar et al. (2019)					∘		∘		∘		∘	•				
Cruz et al. (2016)								∘			∘	•				
Bigheti et al. (2019b)			∘				∘			∘		•				
Tasci et al. (2018)			∘			∘			∘			•		∘		
Gilani et al. (2016)			∘			∘	∘				•	∘				
Givehchi et al. (2014)			∘								•					
Ahmed and Roy (2016)							∘						•			
Lim et al. (2016)						∘							•			∘
Garimella (2018)						∘	∘						∘	•	∘	
Murray et al. (2017)							∘						∘	•	•	
Park and Wook Jeon (2019)					∘		∘							•		

9.2.2. Protocols

The integration of SCADA with both industrial legacy systems and IT-layer tools, such as SAP, MES, and ERP, is one of the fundamental challenges for embarking on a path of convergence of the IT/OT layers. In this field, such integration can be conveyed by the adoption of lasting and compatible standardized protocols, such as those implementing the IEC 61850 and/or the IEC 104 directives, instead of proprietary ones, or the adoption of middlewares for enabling the communication between IT applications and OT field devices, for example, to translate protocols and commands (Garimella, 2018; Park and Wook Jeon, 2019). The integration of control systems such as SCADA/DCS with the whole software set used at the IT level highlights the importance of dealing with security practices for IT/OT integration. An approach described in literature adopts the Hofstede's organizational culture theory for integrating modern systems. This theory foresees the adoption of a framework for cross-cultural communication that relates the corporate departments with the cultural classes according to Hofstede's theory. This approach shows that modern integration systems must plan to aggregate the knowledge of the workers of both departments to implement a successful strategy for cybersecurity and for all the concerns of IT/OT convergence (Murray et al., 2017).

9.3. Advanced Industrial Control Systems wrap-up

Table 4 provides a synthetic view of the literature works addressing the Advanced Industrial Control Systems. Most of the works propose solutions based on the distributed management of the assets available in the production sites.

On one side, the scientific community that investigates production plant control puts much focus on software programmable controllers, so to study their behavior through simulations and determine the right deployment for new use cases such as the employment of deterministic communication and SDN/NFV at lower layers. While PLC virtualization is widely adopted, most related works favor on-premise deployment of virtualized PLCs over off-premise alternatives. This preference likely stems from a lower trust level put by companies in sharing critical core data/resources over widely accessible networks.

On the other side, recent technological advancements in Industrial Control Systems (ICS) aim to facilitate IT and OT management and convergence. This is achieved through the use of Advanced Distribution Management Systems (ADMS), advanced SCADA systems, and interoperable strategies, such as those suggested by standardized protocols and tools designed to overcome hardware vendor-specific limitations. Despite these efforts, vendor-specific approaches remain a significant challenge, often slowing down the progress of IT/OT convergence. The use of interoperability protocols, like the OPC UA and the IEC 61850, is the main trend in connecting the components of the shop floor with each other and with complex ICS.

Table 4 might seem to suggest a lack of emphasis on information security. However, these works primarily focus on systems that are either on-premise or operate within secure company networks, such as private LANs or VPNs, where security measures are inherently managed within the controlled environment. As reported in Section 10, several works address cybersecurity from the ICS systems perspective.

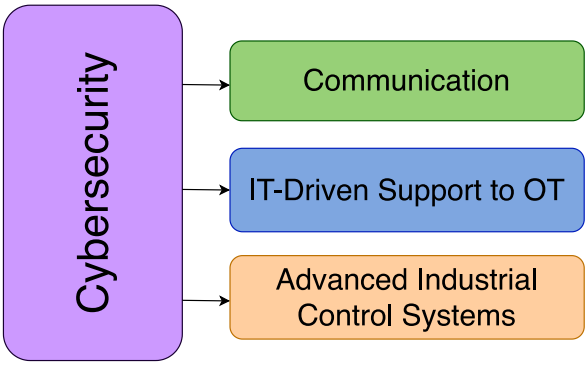

Fig. 12. Cybersecurity taxonomy.

10. Cybersecurity taxonomy

Our survey has revealed that cybersecurity is a consistently emphasized concern among researchers. Regardless of the specific aspect of integration being addressed, there is a shared understanding that any advancements aimed at bringing IT and OT closer together must confront the security challenges inherent in such convergence (see Tables 2–4).

Security and safety are critical priorities in the industrial sector. Industrial sites and factory plants generate highly sensitive information and house critical assets essential to the business operations of any company. Ensuring the confidentiality, integrity, and availability of data exchanged in OT is crucial for employee safety and enterprise privacy. Traditionally, the OT layer operated in isolation from enterprise networks, restricting potential attacks to physical or close-proximity scenarios. However, the convergence with the IT layer has significantly expanded the attack surface, resulting in a growing number of cyberattacks targeting ICSss like SCADA/DCS systems (https://us-cert.cisa.gov/ics). Protecting enterprise assets and maintaining controlled access are among the most pressing concerns in I4.0/5.0 (Internet of Things (IoT), 2021; Filkins et al., 2019; Casola et al., 2022; Fortinet, 2019).

While the works discussed in the previous sections have addresses security only superficially, this section discusses state-of-the-art research that places security aspects of the integration at the core of the investigation. To present these works systematically, we approach the cybersecurity literature from three essential perspectives, each referring to a foundational concept of our taxonomy tree. Ultimately, in our taxonomy, cybersecurity is not considered an individual realm but rather a concept that permeates and cross-cuts the integration domain presented thus far (see Fig. 12).

10.1. Communication

A closer interaction between IT and OT layers introduces the potential for IT-specific security threats to impact the physical world. This propagation can be critical, exposing the supply chain, production lines, and enterprise systems to significant risks. To address this issue,

the research community is actively investigating potential attacks and vulnerabilities that could propagate to the OT domain.

The first line of defense in protecting industrial shop floor entities is adopting a security-by-design approach, as advocated by GDPR and Network and Information Security (NIS) directives. This approach emphasizes integrating cybersecurity considerations when purchasing or redesigning IT or OT systems. A widely recognized best practice for designing convergent IT/OT networks involves segmenting the network into logical realms and defining strict rules for data and entity access and communication within each segment. Additionally, the deployment of next-generation firewalls (NGFW) is essential. These advanced firewalls can identify OT application protocols by passively analyzing network traffic, including encrypted traffic. They also provide critical features such as network filtering, physical device profiling, and classification, ensuring enhanced security for IT/OT convergent infrastructures (Heritage, 2019; Internet of Things (IoT), 2021; Fortinet, 2019).

In addition to designing the communication architecture, a critical focus is placed on communication protocols and encryption, particularly when extending communication to remote industrial sites and assets. Industrial DERs is an example of a remote asset working on MODBUS that might suffer security threats. A valuable solution provided by technological advancements to ensure low-overhead end-to-end AES encryption on MODBUS communications is the deployment of hardware cryptographic acceleration chips at both ends of the communication. This approach helps secure the transmission and prevent exposure of MODBUS data. Generally, modern IIoT devices and assets are capable of supporting low-level security features, but implementing these security measures can be challenging due to the fluid nature of device security boundaries and the inherent dynamism of IIoT devices. This makes securing encryption processes in such environments a complex task (Hupp et al., 2020; Leander et al., 2019).

Overall, the convergence of IT and OT brings security risks because of the multitude of heterogeneous technologies, protocols, standards, and buses involved. In Figueroa-Lorenzo et al. (2020), a framework is proposed that help operators assess the security of industrial plants and enterprise systems, thus boosting the adoption of security practices to modern I4.0/5.0 oriented factories (Figueroa-Lorenzo et al., 2020).

10.2. IT-Driven support to OT

The first approach to maintaining the security and boundaries of a company's domain is to apply a set of security and privacy best practices and strategies. The initial step in this direction is to educate and train employees on cybersecurity to safeguard both IT and OT layers, as well as on security policies for sharing information between departments. IT departments need to be aware of the functionalities of the underlying devices, while OT personnel should be educated on the security practices that the IT world has extended to all network-connected devices. To bridge the knowledge gap and gain a comprehensive understanding of the different strategies used to protect the IT and OT layers, the Industrial CyberSecurity 4.0 (InCyS 4.0) research program offers open-source educational materials and high-quality courses aimed at enhancing employees' cybersecurity skills (Yonemura et al., 2018; Karampidis et al., 2019).

Secondly, the best widespread recognized way to protect the modern industrial systems is to adopt the so-called "defence-in-depth" strategy. It is a multi-layered holistic approach to secure an integrated industrial IT/OT convergent architecture. This strategy adopts several different methods, such as antivirus/malware software, secure/biometric authentication, use of demilitarized zones, firewalls, intrusion detection systems (IDSs), etc., which together can provide a strong defense path across all levels (Paes et al., 2020; Filkins et al., 2019).

To avoid the installation of complex and expensive firewalls, in modern industrial scenario a data diode technique can be used. This technique exploits a single-direction serial data channel connecting devices at different levels. A transmit hardware is the only connection between the transmitter gateway and the receiver gateway, there is no receiving line so there will not be any exchange of data back into the control system (Manson and Anderson, 2019).

A further step towards achieving full cybersecurity in modern industrial environments envisage leveraging techniques and practices of Big Data processing. In this direction, many proposals suggest ML-based techniques to improve the overall system security. In particular, the adoption of ML techniques found room in advanced Intrusion Detection System (IDS) systems applied to ICS, where ML models are instrumented to analyze the network traffic and detect malicious behaviors. This approach is promising but still suffer of training dataset problems. Since there still is a relatively low number of attack samples compared to the massive amount of normal traffic flowing through the network, traditional ML algorithms can lead to many false negatives (Bhamare et al., 2020).

One more interesting IT-driven solution for industrial cybersecurity is the *blockchain*. Blockchain offers flexibility across multi-layer architectures and can be applied to a wide range of heterogeneous devices. However, its adoption may lead to performance and scalability issues, potentially slowing down systems. Additionally, blockchain alone cannot replace other essential security mechanisms such as firewalls, encryption, and authorization; these must still be implemented alongside blockchain to ensure comprehensive security. Among others, a Direct Acyclic Graph (DAG) structured blockchain proved to be the best option in modern industrial IT/OT converging environments (Ram Kumar et al., 2020; Minoli and Occhiogrosso, 2018).

Finally, implications for industrial security might be also caused by flaws present in the design of new products. There are safety guidelines that address this aspect from a semantic perspective (Giehl and Wiedermann, 2018).

10.3. Advanced Industrial Control Systems

The integration of information technology, physical, and cyber components increases the complexity of the CPS system, sometimes making it a highly distributed system exposed to severe security risks. On this direction, a taxonomy can help companies to undertake the transition to an IT/OT convergent scenario, in terms of knowledge of the domain, the main threats, their consequences, and possible countermeasures to take (Murray et al., 2017; Gawanmeh and Alomari, 2018).

The first effective defense for industrial control systems is to detect malicious behavior through an IDS. A valuable solution could involve deploying an IDS on a fog node close to the OT level, incorporating both signature-based and anomaly detection sub-components. The signature-based component functions similarly to antivirus software, relying on predefined rules, and triggers an alert when a violation occurs. In contrast, the anomaly detection component can identify deviations from normal behavior, helping to detect new, previously unknown threats (Colelli et al., 2019).

In OT, a critical cybersecurity concern lies in the low-level communication protocols which are typically based on a request/response approach. These protocols can expose vulnerabilities to three types of attacks: man-in-the-middle (MITM), denial of service (DoS), and PLC reprogramming attacks. In these protocols, malicious actors could intercept and decrypt packets exchanged at the data link and network layers, potentially executing more sophisticated attacks like ARP poisoning. To counter these risks, one of the most promising solutions is the deployment of a network Intrusion Detection System (NIDS) to detect malicious traffic between authorized entities. Deep Packet Inspection (DPI) tools and firewalls are also employed to protect the traffic based on TCP/IP, whereas data diodes can be useful to build a one-way gateway for data and commands sent to the PLCs (Rosa et al., 2019). The last aspect of IO/OT convergent systems that can expose vulnerabilities to malevolent agents is the integration and the interoperability of legacy systems, devices and protocols. Legacy devices have limited

Table 5
Literature contributions to 'Cybersecurity'. Symbols: • denotes substantial focus; ∘ indicates marginal discussion.

[#]	IT-Driven support to OT					Communication						Advanced ICSs				Cybersecurity	HC
	Processing strategies		Provisioning models			Northbound				Southbound		Software-defined Control		Distributed Control			
	Model-Driven	Data-Driven	Cloud	Fog	Edge	Comm. Pat.	Transp	Net	MC	Non MC		Off Premise	On Premise	Architectures	Protocols		
Sandberg and Hunter (2017)																•	
Manner (2019)																•	
Prinsloo et al. (2019)			∘				∘							∘		•	∘
Hassanzadeh et al. (2020)			∘				∘					∘	∘	∘	∘	•	
Murray et al. (2017)							∘								∘	•	
Paes et al. (2020)						∘	∘		∘						∘	•	
Hupp et al. (2020)							∘									•	
Bhamare et al. (2020)	∘												∘		∘	•	
Colelli et al. (2019)				∘			∘						∘		∘	•	
Yonemura et al. (2018)																•	
Giehl and Wiedermann (2018)														∘		•	∘
Sajjadi and Niknia (2013)														∘		•	
Karampidis et al. (2019)																•	
Leander et al. (2019)						∘									∘	•	
Rosa et al. (2019)						∘	∘								∘	•	
Manson and Anderson (2019)	∘															•	
Heritage (2019)							∘									•	
Minoli and Occhiogrosso (2018)						∘										•	
Ram Kumar et al. (2020)						∘										•	

computation power, and adding security mechanisms might cause a non-negligible overhead. Client/server legacy protocols could be prone to tampering from external malicious agents, because of the clear-text communication and open ports. As a viable solution to these integration issues, companies should equip devices and update protocols with encryption/authentication features, otherwise it is better not to expose them (Manner, 2019; Sandberg and Hunter, 2017).

Finally, three valuable vertical examples, targeting controls of water supply, power grid management, and industrial 3D printing domain, are worth mentioning. In all verticals, it is stressed the importance of detecting malicious behaviors at OT level through continuous monitoring and an adaptive security approach. By constantly observing the system and adjusting security measures in real-time, it becomes possible to detect and mitigate threats promptly, minimizing the impact of potential attacks on critical industrial operations (Hassanzadeh et al., 2020; Sajjadi and Niknia, 2013; Prinsloo et al., 2019).

10.4. Cybersecurity wrap-up

In Table 5, we reported an analysis of the literature addressing cybersecurity in modern industrial systems. From those studies, it has become evident that companies require a holistic approach to address cybersecurity challenges in IT/OT convergence scenarios. A significant obstacle to implementing IT/OT convergence lies in the need for departments to adapt to new responsibilities that were previously outside their purview. This is particularly true for OT departments, which traditionally operated independently of IT with their own established security protocols. Achieving integration between IT and OT divisions is essential to foster a shared understanding of security measures within the convergent system, thereby breaking down organizational silos. Furthermore, effective collaboration among OT software developers, machine vendors, and network architects is crucial for safeguarding production assets.

Many approaches focus on assets used in production sites and complex industrial control systems, emphasizing the analysis of networking protocols and their associated vulnerabilities. The reports also highlight the importance of protecting legacy equipment still in use at production sites while ensuring its seamless integration during the transition. Addressing this challenge is an area where IT techniques show promise, aiming to fulfill the security requirements for information exchange between IT and OT departments. Among the surveyed works, a few contributions stand out for addressing the need for employee upskilling and reskilling during the Industry 5.0 transition, which prioritizes human centrality, sustainability, and resilience as its core pillars.

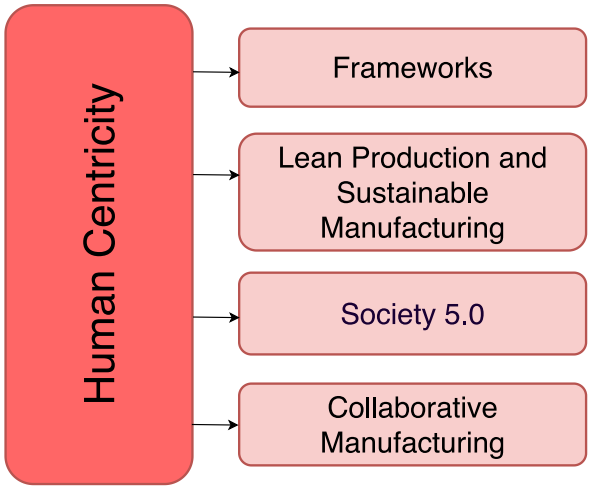

Fig. 13. Human centricity taxonomy.

11. Human centricity taxonomy

In the rapidly evolving landscape of the modern industry, the concept of human centricity has emerged as a focus area. Human centricity in industrial contexts prioritizes the needs, capabilities, and well-being of workers, integrating human factors into the design and implementation of technologies and processes. This approach contrasts with traditional models that often emphasized efficiency and productivity at the expense of the worker's satisfaction and safety.

The integration of IT and OT layers in modern industrial scenarios presents significant opportunities for enhancing industrial efficiency and innovation. However, ensuring a human-centered integration is essential for achieving sustainable and ethical advancements. Human Centricity is one of the pillars of the Industry 5.0 paradigm, which addresses the complex interplay between technology and human factors in the aim of creating integrated IT/OT systems that not only drive industrial progress, but also support and enhance the human workforce at their core (see Table 6).

We conducted a literature review to identify and analyze proposals that highlight and discuss the central role of the human being in the digital transformation processes shaping the industrial sector. For the surveyed works, we propose the classification depicted in Fig. 13.

The first research thread focuses on the definition of a novel concept that embraces both the Industry and the whole modern society, i.e., Society 5.0 (S5.0) (Huang et al., 2022; Nair et al., 2021; Kasinathan et al., 2022). Society 5.0 aims to integrate advanced IT technologies like AI, IoT, and robotics into all aspects of the human life, with the purpose of guaranteeing a balanced, inclusive, and sustainable

Table 6
Literature contributions to 'Human Centricity'. Symbols: • denotes substantial focus; ∘ indicates marginal discussion.

[#]	IT-Driven support to OT					Communication						Advanced ICSs				Cybersecurity	HC
	Processing strategies		Provisioning models			Northbound				Southbound		Software-defined Control		Distributed Control			
	Model-Driven	Data-Driven	Cloud	Fog	Edge	Comm. Pat.	Transp	Net	MC	Non MC		Off Premise	On Premise	Architectures	Protocols		
Huang et al. (2022)	∘																•
Nair et al. (2021)	∘	∘	∘	∘	∘											∘	•
Kasinathan et al. (2022)		∘	∘													∘	•
Mourtzis et al. (2022)	∘	∘	∘		∘											∘	•
Grosse et al. (2023)																	•
Carayannis et al. (2024)																	•
Ivanov (2023)		∘								∘						∘	•
Longo et al. (2020)	∘																•
Modoni and Sacco (2023)	•	∘															•
Castillo et al. (2021)												∘	∘			∘	•
Kadir et al. (2018)																	•
Sahan et al. (2023)																	•
Adel (2022)		∘	∘													∘	•
Weiss et al. (2021)												∘	∘	∘			•
Javaid et al. (2022)																	•
Cohen et al. (2022)													∘	∘			•
Adriaensen et al. (2022)												∘	∘	∘			•
Liu et al. (2024)		∘										∘	∘				•
Souza et al. (2022)																	•
Moraes et al. (2023)																	•
Eriksson et al. (2024)																	•
Rahardjo et al. (2024)	∘	∘															•
Rannertshauser et al. (2022)		∘															•

society. Central to this vision is the collaboration between humans and machines as a key to enhance human creativity, quality of the decision-making, working conditions, as well as fostering innovation. This approach ensures that technological advancements expand their boundaries to benefit society as a whole, addressing challenges like aging populations, environmental sustainability, and economic inequality, while promoting overall well-being. In this context researchers have highlighted challenges, opportunities and impact of this concept on modern industries (Mourtzis et al., 2022; Grosse et al., 2023).

In the context of S5.0, researchers have proposed frameworks that provide guidelines for integrating techno-centric and human-centric innovations. Specifically, these guidelines illustrate how the synergy between IT-driven technological advancements and human-centricity principles can bring a significant added value (Carayannis et al., 2024; Ivanov, 2023). This added value has been proved by two relevant studies in literature. The first one propose a Value Sensitive Design (VSD) approach based on human–machine symbiosis in the Factory of the Future. The proposed solution enables and supports the human operator in designing and developing their industrial project through the Augmented Reality. The second one authors developed a human digital-twin-based platform that promotes harmonization and orchestration between humans and machines through the monitoring, simulation, and optimization of their interactions, thus enhancing performances and efficiency (Longo et al., 2020; Modoni and Sacco, 2023).

The collaboration between Humans and Machines, meant as Robots, is central to the Human Centricity principle. The research threads that investigate Cobots (Collaborative Robots) addresses all the scenarios in which robots and humans work side by side in a shared workspace. Unlike traditional industrial robots, which typically operate in isolation to ensure safety, cobots are equipped with advanced sensors and AI-based capabilities that enable them to interact safely and efficiently with human workers (Castillo et al., 2021; Kadir et al., 2018; Sahan et al., 2023). Some research efforts in the field explore the socio-technical environment of Industry 4/5.0 involving cobots at the individual, team, and organizational levels (Adel, 2022; Weiss et al., 2021). In such environments, cobots are often deployed in assembly lines, in picking station for collaborative loading and unloading of objects, and/or in environments dangerous for the humans (Javaid et al., 2022; Cohen et al., 2022; Adriaensen et al., 2022; Liu et al., 2024).

Along with the technological advancement of the production lines, in human-driven activities of modern industrial environments the concept of lean production has taken place. Lean production is a systematic manufacturing methodology aimed at minimizing waste and maximizing efficiency within production processes. Key principles of Lean Production include identifying customer value, mapping the value stream, ensuring smooth production flow, employing a pull system driven by demand, and pursuing continuous improvement. This methodology boosts productivity, reduces costs, and enhances product quality (Souza et al., 2022; Moraes et al., 2023), aligning seamlessly with the goals of Industry 5.0. These principles have been extensively studied and applied across various industrial contexts. Recent research delves into the complexities of managing concurrent organizational changes during digital transformation toward Industry 5.0. A notable study investigates how Lean Production practices and Industry 4.0 technologies can coexist to improve manufacturing operations in the Industry 5.0 era. Similarly, a recent sustainable innovation framework (SIF) has been proposed, leveraging inductive and integrative approaches based on Lean Production and Industry 5.0 technologies to achieve process excellence. The application of Lean Production emphasizes the critical role of operators and engineers in production processes, optimizing workflows, routines, decision support, and information exchange. One prominent area of implementation is production planning, where this approach helps overcome errors arising from misinterpretations due to human cognitive biases (Eriksson et al., 2024; Rahardjo et al., 2024; Rannertshauser et al., 2022).

12. Final discussion and lesson learnt

This section presents a critical examination of the survey's qualitative and quantitative findings. In addition, it underscores several key challenges related to IT/OT integration, which, in our view, deserve to be prioritized within the future research agenda.

The taxonomic approach discussed in Sections 7–11 provides the reader with an overview of the state of the art on the broad theme of IT/OT convergence. According to the followed approach, each research contribution belongs to one specific branch of the taxonomy tree, but it can also touch on topics addressed by other branches. In Table B.7, we propose a comprehensive view of all the surveyed works. Each row depicts a contribution along with the taxonomy concepts that the contribution itself either addresses as a primary concern or just touches on.

At first glance, if we just consider primary concerns, the majority of collected works fall under the *Communication* and *IT-Driven support to OT* branches, proving that these are the realms where research communities are pushing hard towards the achievement of convergence. These taxonomies almost double the count of papers found in the Advanced Industrial Control Systems branch. Such a strong polarization also suggests that the integration process is receiving little push from OT-focused research. The reason lies in the skepticism exhibited by the OT research communities towards fully opening the OT boundaries to external systems, despite the wide range of technologies, tools, and solutions provided by IT to strengthen cybersecurity.

On the Communication side, there is an abundance of integration solutions that rely on Communication pattern mechanisms (mostly

based on IIoT protocols) (Figueroa-Lorenzo et al., 2020; Stratogiannis and Gkiala-Fikari, 2018; Bosi et al., 2020; Benedick et al., 2019; Nguyen-Hoang and Vo-Tan, 2019). IIoT protocols are known to offer an asynchronous transfer of data among decoupled systems, thus implementing some form of loose integration between participants. Some of the works falling in the mentioned category also rely on the Cloud Computing paradigm to implement their proposed solutions. With a count of 36 papers, the Communication pattern leaf is the most numerous in the Communication taxonomy. A handful of works explore the problem at the Transport layer (Pokhrel and Garg, 2021; Internet Engineering Task Force (IETF), 2024; Samitier, 2017; Felser et al., 2019), while a few have devised innovative solutions in the Networking layer (Yannuzzi et al., 2017; Shrestha and Lin, 2020; Kupzog et al., 2020; Thames and Schaefer, 2016) by leveraging the configurability and adaptability features of *software-based networking* to build a common communication framework where IT and OT can converge. Again, while virtual networking is extensively adopted in many verticals, in the industrial sector the opening and sharing of OT networks with IT departments is still contrasted.

In regards to Southbound, literature efforts are almost evenly split between Mission-critical protocols (Lo Bello and Steiner, 2019; Bruckner et al., 2019; Cavalcanti et al., 2019; Gutiérrez et al., 2017; Pop et al., 2018; Dujovne et al., 2014; Accettura et al., 2015) and Non mission-critical protocols (Liu et al., 2019; Amendola et al., 2017; Yi et al., 2017) environments. In particular, Mission-critical protocols protocols are an interesting topic for researchers, who claim that IT can provide valid support to the time-critical processes that run in work machine contexts.

Researchers are calling on both model-driven and data-driven computation strategies to devise effective solutions that support the convergence of OT and IT. Many are experimenting with AI/ML/DL to propose smart systems and applications that can improve the production process (Borghesi et al., 2021; Akira Kanazawa, 2019; Gahlawat et al., 2023; Hicham et al., 2023; Nian et al., 2020; Kegyes et al., 2021; Sajitha et al., 2024; Ameri et al., 2024). Most of these solutions focus on solving issues of OT assets, such as anomaly detection and predictive maintenance, while a few extend the potential of AI to more sensitive phases of production, such as the control loop. Although there has been some openness from factory owners to share machine (big) data for feeding these applications, they remain reluctant to tear down shop floor boundaries to accommodate incoming stimuli from the external environment. In that respect, the Edge provisioning model seems appealing not only for the capability of supporting mission-critical applications (Jiang and Wan, 2021; Bellavista et al., 2024b; Tazzioli et al., 2024), but especially for the guarantees that sensitive data never leaves the factory premises. Despite they are unfit for dealing with delay-sensitive applications, the Cloud/Fog remains the only viable path when huge and scalable computing power is requested, like in the case of running complex model-driven Digital Twins (Dietz and Pernul, 2020; Bécue et al., 2020) or training DL models (Deng et al., 2022; Liu et al., 2021; Sajitha et al., 2024; Ameri et al., 2024). Semantics are believed to be among the technologies called upon to favor IT/OT convergence. Among the surveyed works, one proposes to unify some existing ontologies to build a more comprehensive one capable of covering the broad domain of resource management and allocation in IoT environments (Koorapati et al., 2018). Some explore the opportunity of leveraging semantics in the Power Grids vertical domain (Stratogiannis and Gkiala-Fikari, 2018; Doğdu et al., 2014; Souvent et al., 2019) with the purpose of having a common ground on which heterogeneous process control systems can exchange data (indeed, in the table Advanced Distribution Management Systems (ADMS) is indicated as a minor focus). Finally, network level QoS is explored by introducing a semantic representation of the capabilities of *Things* that expose their services on the network (Sciullo et al., 2020).

Compared with the above-mentioned taxonomy branches, the smaller number of literary works targeting the Advanced Industrial Control Systems highlights that the exploration of integration solutions at the shop floor layer is lagging behind.

The integration of legacy systems and protocols employed on the shop floors is a very requested feature in the I4.0 transition (Givehchi et al., 2017; Bellavista et al., 2019; Bosi et al., 2019). Unfortunately, most of OT assets were not designed to be connected to any network so they cannot interact with modern communication protocols largely deployed in IT environments. The research community seems cautious about proposing remotely deployed Software-defined Control controllers (only two contributions were found in that respect), while it seems keener to advise on-premise softwarized controllers, as witnessed by a handful of papers (Badar et al., 2019; Cruz et al., 2016; Bigheti et al., 2019b; Tasci et al., 2018). Some have tackled the integration problem from a higher perspective, claiming that the convergence towards IT needs to be realized by means of ADMS (Ahmed and Roy, 2016; Lim et al., 2016), which are information aggregators by nature and are indeed prone to integration. Finally, a few works investigated the interoperability of industrial protocols in SCADA environments as an enabler of the convergence aforementioned (Garimella, 2018; Murray et al., 2017; Park and Wook Jeon, 2019). For sure, one of the barriers preventing the extensive digitization of assets operating on the shop floor is the potential cyber-attacks that could be unleashed by letting IT penetrate OT.

Human centricity, a cornerstone of Industry 4.0 and 5.0, marks a paradigm shift by prioritizing human needs and well-being in industrial advancements. By integrating IT and OT systems, human-centric frameworks like Society 5.0 leverage technologies such as AI, IoT, and robotics to address societal challenges like aging populations and environmental sustainability, while enhancing decision-making and innovation (Huang et al., 2022; Carayannis et al., 2024; Grosse et al., 2023). Tools like Value Sensitive Design (VSD) and human digital twins exemplify this principle. VSD enables augmented reality-based design, while digital twins harmonize human–machine interactions, improving efficiency and collaboration (Longo et al., 2020; Modoni and Sacco, 2023). Similarly, collaborative robots (cobots), equipped with advanced sensors and AI, facilitate safe and efficient human–robot collaboration in shared workspaces, transforming tasks from assembly lines to hazardous environments (Castillo et al., 2021; Longo et al., 2020). Lean production principles further support human-centricity by minimizing waste and enhancing production planning, aligning with Industry 5.0's goals of sustainability and process excellence. Recent studies demonstrate how these methodologies coexist with Industry 4.0 technologies to optimize workflows and mitigate human cognitive biases (Souza et al., 2022; Eriksson et al., 2024). In conclusion, human-centricity harmonizes technological advancements with human needs, fostering inclusive, ethical, and efficient industrial transformation. By embedding these principles into processes and addressing societal challenges, Industry 5.0 positions workers as central to sustainable industrial innovation.

Finally, it is worth mentioning the most critical aspect that the integration process has been facing, i.e., the security to build around production data and the safety to be assured for OT assets and the workforce. Cyber-security is a topic that deserves the attention of around 90% of the surveyed proposals, independently of whether security was dealt as a major or as a minor target, thus witnessing that the concern of research communities towards security and safety threats is huge (Paes et al., 2020; Bhamare et al., 2020; Manson and Anderson, 2019; Ram Kumar et al., 2020; Minoli and Occhiogrosso, 2018; Giehl and Wiedermann, 2018; Karampidis et al., 2019; Yonemura et al., 2018; Filkins et al., 2019; Heritage, 2019; Fortinet, 2019; Internet of Things (IoT), 2021; Hupp et al., 2020; Figueroa-Lorenzo et al., 2020; Leander et al., 2019; Hassanzadeh et al., 2020; Sajjadi and Niknia, 2013; Colelli et al., 2019; Gawanmeh and Alomari, 2018; Manner, 2019; Rosa et al., 2019; Sandberg and Hunter, 2017; Murray et al., 2017; Prinsloo et al., 2019). What emerged from this survey is that, despite several promising proposals being made, further investigation

and experimental initiatives need to be taken to guarantee that security mechanisms developed by IT communities can assure the same quality level in environments subject to severe risks like the industrial control systems, where an undetected intrusion could lead to dire consequences for the factory assets and for people at work. The feeling we have at the end of the study is that if big to mid companies have many resources to invest in cyber security, small companies might not be able to afford it, and therefore are not yet ready for a full transition to digital.

We conclude with some synthetic considerations on the current status of integration and the main future research perspectives. We have observed an abundance of works that address communication aspects to enable IT/OT integration. Despite the research value of the analyzed research proposals, we believe that the presence of many legacy industrial control systems and the widespread spread of proprietary communication protocols still constitutes a big barrier to integration, so more attention must be put on the topic. A lot of proposals, both directly and indirectly, push for enhancing cybersecurity as a key to easier integration of the factory departments. The feeling is that comprehensive and viable defensive approaches have not yet been devised. The abundance of operational data made available at the business departments, along with the strong support of robust and mature Information Technologies like, e.g., semantics, AI, and Edge/Cloud computing, enables a looser yet effective form of integration between the OT and IT environments. Edge computing, in particular, enables the execution of softwarized industrial appliances (e.g., virtual PLCs) within the factory domains and meets the strict requirements of trustworthiness, security, and mission-criticality that are imposed in industrial settings. Finally, a strong need has emerged to retrain employees of the IT and OT departments to raise awareness over the convergence aspects. Convergence inevitably leads to adopting practices and technologies unusual for those environments. It is therefore compulsory that the two departments build a shared knowledge base and reach a common understanding of the convergent system, which is no longer confined to separate areas of the company.

13. Concluding remarks

The momentum gained by the fourth industrial revolution is witnessed by the innumerable initiatives run by authoritative standardization bodies to push new standards that could be adopted worldwide, huge investments made by national and regional governments to support the digitization of the factory of the future, and an intense research activity carried out by a number of diverse communities. The Industry 4.0 revolution is expected to bring new business opportunities to manufacturing companies, provided that the latter is keen to undertake fast digitization of their assets through enabling IT like 5G, AI, IoT, Edge and Cloud, to name a few.

While IT has seamlessly integrated into companies' managerial departments, offering robust support for business processes, its adoption in operational departments has been hindered primarily by security and safety concerns. Research communities are actively exploring the opportunities that a gradual IT/OT convergence could bring to the industrial manufacturing sector and have proposed numerous innovative approaches to accelerate this integration process. In this paper, we propose a systematic survey of all efforts found in the literature that deal with theoretical, technical, and practical aspects of IT/OT integration. Unlike existing surveys, we have devised a taxonomic perspective that allowed us to organize the collected works in a conceptual framework that reflects the range of technologies currently in use or expected to be adopted in the near future, in both IT and OT departments (see Fig. B.14). Furthermore, to complete the overall convergence picture, we also presented an overview of the main national and international standardization initiatives that are sustaining IT/OT integration. Finally, we devoted one section of the paper to deliver a synthetic view of the surveyed works and made final considerations on the technological trends that are receiving much attention from the community with regard to the convergence topic. In this way, our survey proposes a valuable roadmap inspiring researchers and practitioners in IT/OT convergence implementation, establishing the trends of this important evolution driving the Industry 4.0 transition.

CRediT authorship contribution statement

Riccardo Venanzi: Writing – review & editing, Writing – original draft, Validation, Investigation. **Giuseppe Di Modica:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Investigation, Conceptualization. **Luca Foschini:** Validation, Supervision, Investigation, Formal analysis, Conceptualization. **Paolo Bellavista:** Validation, Supervision, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The co-author, professor Paolo Bellavista, is an Editorial Board Member/Editor-in-Chief/Associate Editor/Guest Editor for this journal and was not involved in the editorial review or the decision to publish this article.

Appendix A. Glossary

Acronyms

AD Anomaly Detection.

ADMS Advanced Distribution Management Systems.

AI Artificial Intelligence.

AMQP Advanced Message Queuing Protocol.

AMR Automated Meter Reading.

ANN Artificial Neural Networks.

BSP Balancing Service Providers.

CBDM Cloud-Based Design and Manufacturing.

CI/CD Continuous integration and developments.

CIM Common Information Model.

CNC Central Network Controller.

CoAP Constrained Application Protocol.

CoCoOn Cloud Computing Ontology.

COTS Commercial Off-The-Shelf.

CPPS Cyber Physical Production Systems.

CPS Cyber Physical Systems.

CRM Customer Relationship Management.

CUC Centralized User Configuration.

DCS Distributed Control Systems.

DER Distributed Energy Resources.

DF Digital Factory.

DL Deep Learning.

DLMS/COSEM Device Language Message Specification/Companion Specification for Energy Metering.

DMS Distribution Management Systems.

DNN Deep Neural Network.

DNP Distributed Network Protocol.

DPI Deep Packet Inspection.

DQN DeepQ-Network.

DRL Deep Reinforcement Learning.

DSCADA Distributed SCADA.

DSO Distribution Service Operator.

DSS Decision Support Systems.

DT Digital Twins.

eMBB enhanced Mobile BroadBand.

EPRI Electric Power Research Institute.

EPS Electric Power Systems.

ERP Enterprise Resource Planning.

GIS Geographic Information Systems.

HRM Human Resource Management.

I4.0 Industry 4.0.

IACS Industrial Automation and Control Systems.

ICSs Industrial Control Systems.

IDS Intrusion Detection System.

IEC International Electrotechnical Commission.

IETF Internet Engineering Task Force.

IIAF Industrial Internet Architecture Framework.

IIC Internet Industrial Consortium.

IIoT Industrial Internet of Things.

IIRA Industrial Internet Reference Architecture.

IMSA Intelligent Manufacturing System Architecture.

IN Industrial Networks.

IoS Internet of Services.

IoT Internet of Things.

ISA International Society of Automation.

ISO International Organization for Standardization.

IT Information Technology.

ITU International Telecommunication Union.

IVI Industrial Value Chain Initiative.

MDMS Meter Data Management System.

MEC Multi-access Edge Computing.

MES Manufacturing Execution Systems.

MIC Made In China.

MIS Manufacturing Information Systems.

ML Machine Learning.

mMTC massive Machine-Type Communication.

MOM Manufacturing Operations Management.

MPTCP Multipath TCP.

MQTT Message Queuing Telemetry Transport.

NFV Network Function Virtualization.

NTN Non-Terrestrial Networks.

OMS Outage Management Systems.

OPC UA OPC Unified Architecture (UA).

OpenADR Open Automated Demand Response.

OPEX OPerating EXpense.

ORMF Ontology-based Resource Management Framework.

OT Operational Technology.

PCS Process Control Systems.

PLC Programmable-Logic Controller.

PLM Product Lifecycle Management.

PM Predictive Maintenance.

RAMI 4.0 Reference Architectural Model Industrie 4.0.

RES Renewable Energy Sources.

RL Reinforcement Learning.

RTU Remote Terminal Unit.

SCADA Supervisory Control and Data Acquisition.

SDCM Software-Defined Cloud Manufacturing.

SDDC Software-Defined Data Centers.

SDN Software-Defined Networking.

SGAM Smart Grid Architectural Model.

SOA Service Oriented Architecture.

SoC System-on-Chip.

SSN Semantic Sensor Network.

TCCD Thing-edge-cloud Collaborative Computing Decision-making.

TSCH Time Slotted Channel Hopping.

TSN Time-Sensitive Networking.

TSO Transmission System Operators.

URLLC Ultra-Reliable Low-Latency Communications.

USEF Universal Smart Energy Framework.

VNF Virtual Network Functions.

WoT Web of Things.

ZDM Zero Defect Manufacturing.

Appendix B. General surveyed works table and IT/OT integration taxonomy map

See Table B.7 and Fig. B.14.

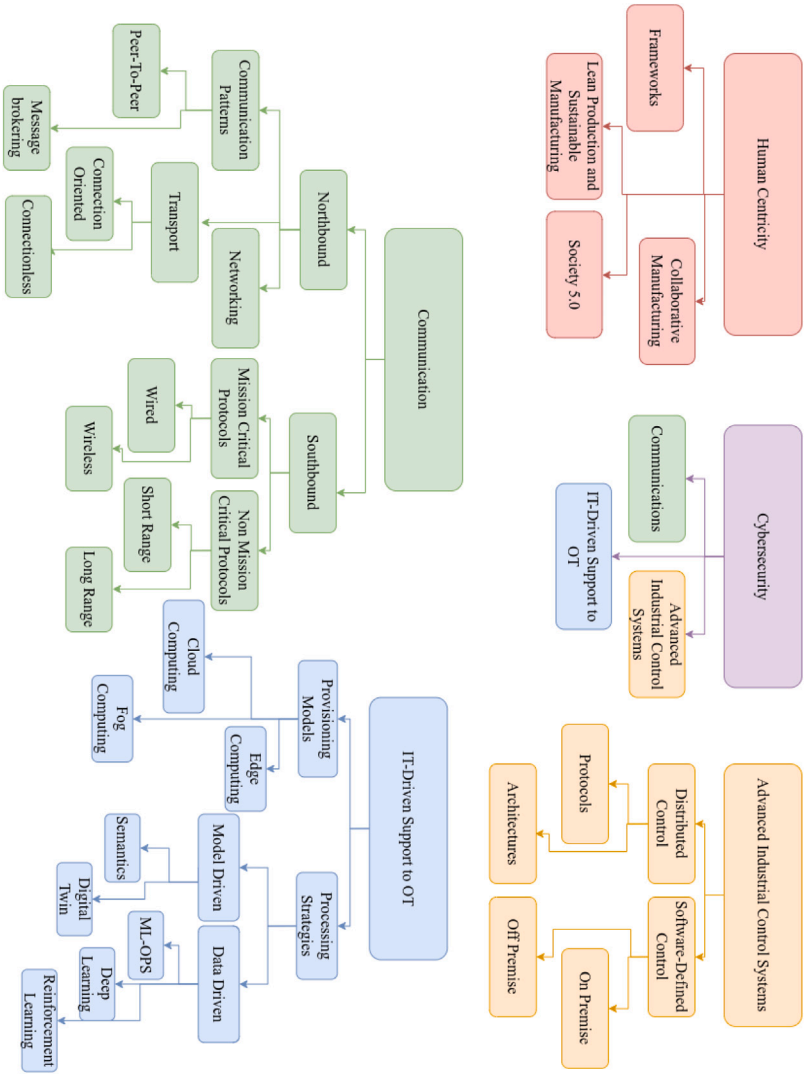

Fig. B.14. IT/OT integration taxonomy.

Table B.7
Comprehensive view of the surveyed works, with main (•) and marginal (∘) topics addressed per work.

[#]	IT-Driven support to OT					Communication					Advanced ICSs				Cybersecurity	HC
	Processing strategies		Provisioning models			Northbound			Southbound		Software-defined Control		Distributed Control			
	Model-Driven	Data-Driven	Cloud	Fog	Edge	Comm. Pat.	Transp	Net	MC	Non MC	Off Premise	On Premise	Architectures	Protocols		
Koorapati et al. (2018)	•		∘	∘	∘			∘					∘		∘	
Doğdu et al. (2014)	•												∘			
Sciullo et al. (2020)	•					∘			∘				∘	∘		
Souvent et al. (2019)	•												∘	∘		
Dietz and Pernul (2020)	•										∘				∘	
Akira Kanazawa (2019)	•										∘					
Singh et al. (2018)	•										∘					∘
Editorial (2020)	•	∘									∘					
Bécue et al. (2020)	•	∘	∘			∘					∘					∘
Borghesi et al. (2021)	•	∘	∘		∘					∘	∘					
Stracener et al. (2019)		•	∘			∘										
Keller (2019)		•	∘													
Bustamante et al. (2023)		•	∘		∘											
Faubel et al. (2024)		•														∘
Venanzi et al. (2023a)		•		∘	∘											∘
Sajitha et al. (2024) and Ameri et al. (2024)		•														
Michailidis et al. (2020)		•	∘	∘	∘	∘		∘		∘			∘		∘	
Deng et al. (2022)		•								∘						
Liu et al. (2021)		•							∘							
Liu et al. (2020)		•											∘		∘	
Gerrikagoitia et al. (2019)			•			∘							∘			
Kavakli et al. (2018) and Montori et al. (2021)			•													
Montori et al. (2023)			•		∘											∘
Jiang and Wan (2021)			•		∘		∘			∘						
Barzegaran et al. (2020)	∘	∘	∘	•					∘				∘	∘	∘	
Pop et al. (2021)	∘		∘	•	∘				∘				∘	∘		
Barzegaran et al. (2019)			∘	•			∘									
Tazzioli et al. (2024) and Bellavista et al. (2024a)			∘		•			∘	∘							
Bellavista et al. (2024b)		∘	∘		•			∘	∘							
Badar et al. (2019)					•				∘		∘		∘			
Stratogiannis and Gkiala-Fikari (2018)	∘					•									∘	∘
Bosi et al. (2020)			∘			•	∘			∘				∘	∘	
Benedick et al. (2019)						•										
Nguyen-Hoang and Vo-Tan (2019)			∘			•	∘									
Pokhrel and Garg (2021)		∘				∘	•			∘						
Morawski and Ignaciuk (2021)							•	∘								∘
Xu et al. (2019)		∘					•	∘								
Wu et al. (2020)		∘					•		∘	∘						
Pokhrel et al. (2021)		∘					•	∘								
Langley et al. (2017)							•	∘								
Fernández et al. (2021)							•	∘		∘					∘	
Yannuzzi et al. (2017)			∘	∘	∘	∘		•			∘				∘	
Shrestha and Lin (2020)			∘		∘	∘		•		∘				∘	∘	
Kupzog et al. (2020)			∘		∘	∘		•			∘		∘			
Thames and Schaefer (2016)			∘			∘		•								
Lo Bello and Steiner (2019)						∘	∘		•	∘				∘		
Bruckner et al. (2019)			∘	∘		∘	∘		•	∘	∘		∘		∘	
Cavalcanti et al. (2019) and Gutiérrez et al. (2017)						∘			•	∘						
Pop et al. (2018)			∘	∘		∘			•							
Vilajosana et al. (2020)						∘	∘		∘	•					∘	
Dujovne et al. (2014)						∘				•					∘	
Accettura et al. (2015)						∘				•						
Yi et al. (2017)			∘				∘			•			∘	∘	∘	
Liu et al. (2019)	∘		∘			∘		∘		•						
Amendola et al. (2017)						∘				•					∘	
Badar et al. (2019)					∘		∘		∘		∘	•				
Cruz et al. (2016)								∘			∘	•				
Bigheti et al. (2019b)			∘				∘			∘		•				
Tasci et al. (2018)			∘			∘			∘			•		∘		
Gilani et al. (2016)			∘			∘	∘				•	∘				
Givehchi et al. (2014)			∘								•					
Ahmed and Roy (2016)							∘						•			
Lim et al. (2016)						∘							•			∘
Garimella (2018)						∘	∘						∘	•	∘	
Murray et al. (2017)							∘						∘	•	•	
Park and Wook Jeon (2019)					∘		∘							•		
Sandberg and Hunter (2017), Yonemura et al. (2018), Karampidis et al. (2019) and Manner (2019)															•	
Prinsloo et al. (2019)			∘				∘						∘		•	∘
Hassanzadeh et al. (2020)			∘				∘				∘	∘	∘	∘	•	
Paes et al. (2020)						∘	∘		∘					∘	•	
Hupp et al. (2020) and Heritage (2019)							∘								•	
Bhamare et al. (2020)	∘											∘		∘	•	
Colelli et al. (2019)				∘			∘					∘		∘	•	
Giehl and Wiedermann (2018)													∘		•	∘
Sajjadi and Niknia (2013)													∘		•	
Leander et al. (2019)						∘								∘	•	
Rosa et al. (2019)						∘	∘							∘	•	
Manson and Anderson (2019)	∘														•	

(continued on next page)

Table B.7 (*continued*).

Minoli and Occhiogrosso (2018) and Ram Kumar et al. (2020)						○								•	
Huang et al. (2022) and Longo et al. (2020)	○														•
Nair et al. (2021)	○	○	○	○	○									○	•
Kasinathan et al. (2022) and Adel (2022)		○	○											○	•
Mourtzis et al. (2022)	○	○	○		○									○	•
Ivanov (2023)		○						○						○	•
Modoni and Sacco (2023)	○	•													•
Castillo et al. (2021)									○	○				○	•
Kadir et al. (2018), Sahan et al. (2023), Javaid et al. (2022), Moraes et al. (2023), Eriksson et al. (2024), Souza et al. (2022), Grosse et al. (2023) and Carayannis et al. (2024)															•
Weiss et al. (2021) and Adriaensen et al. (2022)									○	○	○				•
Cohen et al. (2022)										○	○				•
Liu et al. (2024)		○							○	○					•
Rahardjo et al. (2024)	○	○													•
Rannertshauser et al. (2022)		○													•

Data availability

No data was used for the research described in the article.

References

Aazam, M., Zeadally, S., Harras, K.A., 2018. Deploying fog computing in industrial internet of things and industry 4.0. IEEE Trans. Ind. Inform. 14 (10), 4674–4682.

ABB, Microsoft, 2019. Guide for starting industrial.

Abraham, A., Kovalev, S., Tarassov, V., Vaclav, S., 2016. Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry". IITI'16, Springer.

Accettura, N., Vogli, E., Palattella, M.R., Grieco, L.A., Boggia, G., Dohler, M., 2015. Decentralized traffic aware scheduling in 6TiSCH networks: Design and experimental evaluation. IEEE Internet Things J. 2 (6), 455–470. http://dx.doi.org/10.1109/JIOT.2015.2476915.

Aceto, G., Persico, V., Pescapé, A., 2019. A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges. IEEE Commun. Surv. Tutor. 21 (4), 3467–3501. http://dx.doi.org/10.1109/COMST.2019.2938259.

Adel, A., 2022. Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas. J. Cloud Comput. 11 (1), 40.

Adriaensen, A., Costantino, F., Di Gravio, G., Patriarca, R., 2022. Teaming with industrial cobots: A socio-technical perspective on safety analysis. Hum. Factors Ergon. Manuf. Serv. Ind. 32 (2), 173–198.

Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., Flinck, H., 2018. Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. IEEE Commun. Surv. Tutor. 20 (3), 2429–2453. http://dx.doi.org/10.1109/COMST.2018.2815638.

Agalgaonkar, Y.P., Marinovici, M.C., Vadari, S.V., Schneider, K.P., Melton, R.B., 2016. ADMS state of the industry and gap analysis. Tech. Rep. http://dx.doi.org/10.2172/1427928, URL https://www.osti.gov/biblio/1427928.

Agustí-Torra, A., Sierra-Guerrero, C.I., Jofre, M., Rincón-Rivera, D., 2025. A simulator for testing and developing scheduling mechanisms in integrated 5G/6G-TSN scenarios. In: 2025 25th Anniversary International Conference on Transparent Optical Networks. ICTON, pp. 1–4. http://dx.doi.org/10.1109/ICTON67126.2025.11125416.

Ahmadi, A., Moradi, M., Cherifi, C., Cheutet, V., Ouzrout, Y., 2018. Wireless connectivity of CPS for smart manufacturing: A survey. In: 2018 12th International Conference on Software, Knowledge, Information Management Applications. SKIMA, pp. 1–8. http://dx.doi.org/10.1109/SKIMA.2018.8631535.

Ahmed, A., Roy, C., 2016. Achieving IT/OT integration with AMI, distribution automation management solutions. In: 2016 Saudi Arabia Smart Grid. SASG, pp. 1–8. http://dx.doi.org/10.1109/SASG.2016.7849688.

Akira Kanazawa, T.S., 2019. Yokogawa's Approach to IT/OT Convergence for Successful Digital Transformation. Tech. Rep., Yokogawa.

Al Jawarneh, I.M., Rosa, L., Venanzi, R., Foschini, L., Bellavista, P., 2025. Efficient parallel processing of big data on supercomputers for industrial IoT environments. Electronics 14 (13), 2626.

Alcaraz, C., Lopez, J., 2022. Digital twin: A comprehensive survey of security threats. IEEE Commun. Surv. Tutor. 24 (3), 1475–1503. http://dx.doi.org/10.1109/COMST.2022.3171465.

Alur, R., 2015. Principles of Cyber-Physical Systems. The MIT Press.

Alves, J., Lima, T.M., Gaspar, P.D., 2023. Is industry 5.0 a human-centred approach? A systematic review. Process. 11 (1), http://dx.doi.org/10.3390/pr11010193, URL https://www.mdpi.com/2227-9717/11/1/193.

Ambrosy, N., Kampa, T., Jumar, U., Großmann, D., 2022. 5G and DetNet: Towards holistic determinism in industrial networks. In: 2022 IEEE International Conference on Industrial Technology. ICIT, pp. 1–6. http://dx.doi.org/10.1109/ICIT48603.2022.10002776.

Amendola, S., Occhiuzzi, C., Marrocco, G., 2017. RFID sensing networks for critical infrastructure security: A real testbed in an energy smart grid. In: 2017 IEEE International Conference on RFID Technology Application. RFID-TA, pp. 106–110. http://dx.doi.org/10.1109/RFID-TA.2017.8098901.

Ameri, R., Hsu, C.-C., Band, S.S., 2024. A systematic review of deep learning approaches for surface defect detection in industrial applications. Eng. Appl. Artif. Intell. 130, 107717. http://dx.doi.org/10.1016/j.engappai.2023.107717.

Amqp home, 2008. AMQP Home, visited on December 30, 2024. URL https://www.amqp.org/.

Anjum, N., Latif, Z., Chen, H., 2025. Security and privacy of industrial big data: Motivation, opportunities, and challenges. J. Netw. Comput. Appl. 237, 104130. http://dx.doi.org/10.1016/j.jnca.2025.104130, URL https://www.sciencedirect.com/science/article/pii/S108480452500027X.

Antonino, P.O., Capilla, R., Kazman, R., Kuhn, T., Schnicke, F., Treichel, T., Bachorek, A., Müller-Zhang, Z., Salamanca, V., 2022. Continuous engineering for industry 4.0 architectures and systems. Softw.: Pract. Exp. 52 (10), 2241–2262.

Arica, E., Powell, D.J., 2017. Status and future of manufacturing execution systems. In: 2017 IEEE International Conference on Industrial Engineering and Engineering Management. IEEM, pp. 2000–2004. http://dx.doi.org/10.1109/IEEM.2017.8290242.

Bachinger, F., Zenisek, J., Affenzeller, M., 2024. Automated machine learning for industrial applications – challenges and opportunities. Procedia Comput. Sci. 232, 1701–1710. http://dx.doi.org/10.1016/j.procs.2024.01.168, URL https://www.sciencedirect.com/science/article/pii/S1877050924001698. 5th International Conference on Industry 4.0 and Smart Manufacturing (ISM 2023).

Badar, A., Lou, D.Z., Graf, U., Barth, C., Stich, C., 2019. Intelligent edge control with deterministic-IP based industrial communication in process automation. In: 2019 15th International Conference on Network and Service Management. CNSM, pp. 1–7. http://dx.doi.org/10.23919/CNSM46954.2019.9012680.

Barzegaran, M., Cervin, A., Pop, P., 2019. Towards quality-of-control-aware scheduling of industrial applications on fog computing platforms. In: Proceedings of the Workshop on Fog Computing and the IoT. In: IoT-Fog '19, Association for Computing Machinery, New York, NY, USA, pp. 1–5. http://dx.doi.org/10.1145/3313150.3313217.

Barzegaran, M., Desai, N., Qian, J., Tange, K., Zarrin, B., Pop, P., Kuusela, J., 2020. Fogification of electric drives: An industrial use case. In: 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation. ETFA, vol. 1, pp. 77–84. http://dx.doi.org/10.1109/ETFA46521.2020.9212010.

Bécue, A., Maia, E., Feeken, L., Borchers, P., Praça, I., 2020. A new concept of digital twin supporting optimization and resilience of factories of the future. Appl. Sci. 10 (13), http://dx.doi.org/10.3390/app10134482, URL https://www.mdpi.com/2076-3417/10/13/4482.

Belenguer, A., Pascual, J.A., Navaridas, J., 2023. GöwFed: A novel federated network intrusion detection system. J. Netw. Comput. Appl. 217, 103653. http://dx.doi.org/10.1016/j.jnca.2023.103653, URL https://www.sciencedirect.com/science/article/pii/S1084804523000723.

Bellavista, P., Bosi, F., Corradi, A., Foschini, L., Monti, S., Patera, L., Poli, L., Scotece, D., Solimando, M., 2019. Design guidelines for big data gathering in industry 4.0 environments. In: 2019 IEEE 20th International Symposium on "a World of Wireless, Mobile and Multimedia Networks". WoWMoM, pp. 1–6. http://dx.doi.org/10.1109/WoWMoM.2019.8793033.

Bellavista, P., Bujari, A., Foschini, L., Sabbioni, A., Venanzi, R., 2024a. A MECApp-aware lifecycle management approach in 5G edge-cloud deployments. In: 2024 33rd International Conference on Computer Communications and Networks. ICCCN, IEEE, pp. 1–6.

Bellavista, P., Dahdal, S., Foschini, L., Tazzioli, D., Tortonesi, M., Venanzi, R., 2024b. Kubernetes enhanced stateful service migration for ML-driven applications in industry 4.0 scenarios. In: 2024 IEEE Annual Congress on Artificial Intelligence of Things. AIoT, IEEE, pp. 25–31.

Bellavista, P., Di Modica, G., 2024. IoTwins: Implementing distributed and hybrid digital twins in industrial manufacturing and facility management settings. Future Internet 16 (2), http://dx.doi.org/10.3390/fi16020065.

Benedick, P.-L., Robert, J., Traon, Y.L., 2019. TRIDENT: A three-steps strategy to digitise an industrial system for stepping into industry 4.0. In: IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society. Vol. 1, pp. 3037–3042. http://dx.doi.org/10.1109/IECON.2019.8927010.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., Meskin, N., 2020. Cybersecurity for industrial control systems: A survey. Comput. Secur. 89, 101677. http://dx.doi.org/10.1016/j.cose.2019.101677, URL https://www.sciencedirect.com/science/article/pii/S0167404819302172.

Bigheti, J.A., Fernandes, M.M., Godoy, E.P., 2019a. Control as a service: A microservice approach to industry 4.0. In: 2019 II Workshop on Metrology for Industry 4.0 and IoT. pp. 438–443. http://dx.doi.org/10.1109/METROI4.2019.8792918.

Bigheti, J.A., Fernandes, M.M., Godoy, E.D.P., 2019b. Control as a service: A microservice approach to industry 4.0. In: 2019 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2019 - Proceedings. IEEE, pp. 438–443. http://dx.doi.org/10.1109/METROI4.2019.8792918.

Bittighofer, D., Dust, M., Irslinger, A., Liebich, M., Martin, L., 2018. State of industry 4.0 across german companies. In: 2018 IEEE International Conference on Engineering, Technology and Innovation. ICE/ITMC, pp. 1–8. http://dx.doi.org/10.1109/ICE.2018.8436246.

Bokhtiar Al Zami, M., Shaon, S., Khanh Quy, V., Nguyen, D.C., 2025. Digital twin in industries: A comprehensive survey. IEEE Access 13, 47291–47336. http://dx.doi.org/10.1109/ACCESS.2025.3551532.

Borghesi, A., Di Modica, G., Bellavista, P., Gowtham, V., Willner, A., Nehls, D., Kintzler, F., Cejka, S., Tisbeni, S.R., Costantini, A., Galletti, M., Antonacci, M., Ahouangonou, J.C., 2021. IoTwins: Design and implementation of a platform for the management of digital twins in industrial scenarios. In: 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing. CCGrid, pp. 625–633. http://dx.doi.org/10.1109/CCGrid51090.2021.00075.

Bosi, F., Corradi, A., Di Modica, G., Foschini, L., Montanari, R., Patera, L., Solimando, M., 2020. Enabling smart manufacturing by empowering data integration with industrial IoT support. In: 2020 International Conference on Technology and Entrepreneurship. ICTE, pp. 1–8. http://dx.doi.org/10.1109/ICTE47868.2020.9215538.

Bosi, F., Corradi, A., Foschini, L., Monti, S., Patera, L., Poli, L., Solimando, M., 2019. Cloud-enabled smart data collection in shop floor environments for industry 4.0. In: 2019 15th IEEE International Workshop on Factory Communication Systems. WFCS, pp. 1–8. http://dx.doi.org/10.1109/WFCS.2019.8757952.

Britton, J., deVos, A., 2005. CIM-based standards and CIM evolution. IEEE Trans. Power Syst. 20 (2), 758–764. http://dx.doi.org/10.1109/TPWRS.2005.846202.

Bruckner, D., Stănică, M.-P., Blair, R., Schriegel, S., Kehrer, S., Seewald, M., Sauter, T., 2019. An introduction to OPC UA TSN for industrial communication systems. Proc. IEEE 107 (6), 1121–1131. http://dx.doi.org/10.1109/JPROC.2018.2888703.

Bustamante, A.L., Patricio, M.A., Berlanga, A., Molina, J.M., 2023. Seamless transition from machine learning on the cloud to industrial edge devices with thinger.io. IEEE Internet Things J. 10 (18), 16548–16563. http://dx.doi.org/10.1109/JIOT.2023.3268771.

Cagnin, R.L., Guilherme, I.R., Queiroz, J., Paulo, B., Neto, M.F.O., 2018. A multi-agent system approach for management of industrial IoT devices in manufacturing processes. In: 2018 IEEE 16th International Conference on Industrial Informatics. INDIN, pp. 31–36.

Cai, N., Wang, J., Yu, X., 2008. SCADA system security: Complexity, history and new developments. In: 2008 6th IEEE International Conference on Industrial Informatics. pp. 569–574. http://dx.doi.org/10.1109/INDIN.2008.4618165.

Caiazzo, B., Di Nardo, M., Murino, T., Petrillo, A., Piccirillo, G., Santini, S., 2022. Towards zero defect manufacturing paradigm: A review of the state-of-the-art methods and open challenges. Comput. Ind. 134, 103548. http://dx.doi.org/10.1016/j.compind.2021.103548, URL https://www.sciencedirect.com/science/article/pii/S016636152100155X.

Cândido, G., Barata, J., Colombo, A.W., Jammes, F., 2009. SOA in reconfigurable supply chains: A research roadmap. Eng. Appl. Artif. Intell. 22 (6), 939–949. http://dx.doi.org/10.1016/j.engappai.2008.10.020, URL https://www.sciencedirect.com/science/article/pii/S0952197608001735, Artificial Intelligence Techniques for Supply Chain Management.

Carayannis, E.G., Canestrino, R., Magliocca, P., 2024. From the dark side of industry 4.0 to society 5.0: Looking "Beyond the Box" to developing human-centric innovation ecosystems. IEEE Trans. Eng. Manage. 71, 6695–6711. http://dx.doi.org/10.1109/TEM.2023.3239552.

Casola, V., De Benedictis, A., Mazzocca, C., Montanari, R., 2022. Designing secure and resilient cyber-physical systems: a model-based moving target defense approach. IEEE Trans. Emerg. Top. Comput. 1–12. http://dx.doi.org/10.1109/TETC.2022.3197464.

Castillo, J.F., Ortiz, J.H., Velásquez, M.F.D., Saavedra, D.F., 2021. COBOTS in industry 4.0: Safe and efficient interaction. Collab. Humanoid Robot. 13.

Cavalcanti, D., Perez-Ramirez, J., Rashid, M.M., Fang, J., Galeev, M., Stanton, K.B., 2019. Extending accurate time distribution and timeliness capabilities over the air to enable future wireless industrial automation systems. Proc. IEEE 107 (6), 1132–1152. http://dx.doi.org/10.1109/JPROC.2019.2903414.

Chen, B., Wan, J., Celesti, A., Li, D., Abbas, H., Zhang, Q., 2018. Edge computing in IoT-based manufacturing. IEEE Commun. Mag. 56 (9), 103–109. http://dx.doi.org/10.1109/MCOM.2018.1701231.

Chen, B., Wan, J., Lan, Y., Imran, M., Li, D., Guizani, N., 2019. Improving cognitive ability of edge intelligent IIoT through machine learning. IEEE Netw. 33 (5), 61–67. http://dx.doi.org/10.1109/MNET.001.1800505.

Chen, C., Zhao, K., Leng, J., Liu, C., Fan, J., Zheng, P., 2025. Integrating large language model and digital twins in the context of industry 5.0: Framework, challenges and opportunities. Robot. Comput.-Integr. Manuf. 94, 102982. http://dx.doi.org/10.1016/j.rcim.2025.102982, URL https://www.sciencedirect.com/science/article/pii/S0736584525000365.

Chi, H.R., Wu, C.K., Huang, N.-F., Tsang, K.-F., Radwan, A., 2022. A survey of network automation for industrial internet-of-things toward industry 5.0. IEEE Trans. Ind. Inform. 19 (2), 2065–2077.

Coap home, CoAP Home, visited on December 30, 2024. URL https://coap.space/.

Cochenour, G., Ochoa, R., Rajsekar, V., 2014. Distribution network model readiness for advanced distribution management systems. In: 2014 IEEE PES T D Conference and Exposition. pp. 1–5. http://dx.doi.org/10.1109/TDC.2014.6863194.

Cogliati, D., Falchetto, M., Pau, D., Roveri, M., Viscardi, G., 2018. Intelligent cyber-physical systems for industry 4.0. In: 2018 First International Conference on Artificial Intelligence for Industries (AI4I). pp. 19–22. http://dx.doi.org/10.1109/AI4I.2018.8665681.

Cohen, Y., Shoval, S., Faccio, M., Minto, R., 2022. Deploying cobots in collaborative systems: major considerations and productivity analysis. Int. J. Prod. Res. 60 (6), 1815–1831. http://dx.doi.org/10.1080/00207543.2020.1870758.

Colelli, R., Panzieri, S., Pascucci, F., 2019. Securing connection between IT and OT: the fog intrusion detection system prospective. In: 2019 II Workshop on Metrology for Industry 4.0 and IoT. MetroInd4.0 IoT, pp. 444–448. http://dx.doi.org/10.1109/METROI4.2019.8792884.

Colombi, L., Brina, M., Vespa, M., Tabanelli, F., Dahdal, S., Bellodi, E., Venanzi, R., Tortonesi, M., Vignoli, M., Stefanelli, C., 2024. Optimizing industry 5.0 machine learning-based applications via synthetic data generation. In: 2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks. CAMAD, IEEE, pp. 1–6.

Consortium, W.W.W., SOAP version 1.2, visited on December 30, 2024. URL https://www.w3.org/TR/soap12/.

Conti, M., Donadel, D., Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. IEEE Commun. Surv. Tutor. 23 (4), 2248–2294. http://dx.doi.org/10.1109/COMST.2021.3094360.

Cruz, T., Simões, P., Monteiro, E., 2016. Virtualizing programmable logic controllers: Toward a convergent approach. IEEE Embed. Syst. Lett. 8 (4), 69–72. http://dx.doi.org/10.1109/LES.2016.2608418.

Da Silva, S.R.B., Vogt, F.G., Cesen, F.R., Luizelli, M.C., Rothenberg, C.E., Patra, G., 2025. Bridging TSN and 5G: Synchronization and flow mapping for smart manufacturing. In: 2025 IEEE 11th International Conference on Network Softwarization. NetSoft, pp. 91–96. http://dx.doi.org/10.1109/NetSoft64993.2025.11080615.

Deng, J., Sierla, S., Sun, J., Vyatkin, V., 2022. Reinforcement learning for industrial process control: A case study in flatness control in steel industry. Comput. Ind. 143, 103748. http://dx.doi.org/10.1016/j.compind.2022.103748.

Dietz, M., Pernul, G., 2020. Unleashing the digital twin's potential for ICS security. IEEE Secur. Priv. 18 (4), 20–27. http://dx.doi.org/10.1109/MSEC.2019.2961650.

Doğdu, E., Murat Özbayoğlu, A., Benli, O., Akınç, H.E., Erol, E., Atasoy, T., Güreç, O., Erçin, Ö., 2014. Ontology-centric data modelling and decision support in smart grid applications a distribution service operator perspective. In: 2014 IEEE International Conference on Intelligent Energy and Power Systems. IEPS, pp. 198–204. http://dx.doi.org/10.1109/IEPS.2014.6874179.

Dujovne, D., Watteyne, T., Vilajosana, X., Thubert, P., 2014. 6TiSCH: deterministic IP-enabled industrial internet (of things). IEEE Commun. Mag. 52 (12), 36–41. http://dx.doi.org/10.1109/MCOM.2014.6979984.

Ebrahimi, M., Baboli, A., Rother, E., 2018. A roadmap for evolution of existing production system toward the factory of the future: A case study in automotive industry. In: 2018 IEEE International Conference on Technology Management, Operations and Decisions. ICTMOD, pp. 274–281. http://dx.doi.org/10.1109/ITMC.2018.8691276.

Editorial, I.G., 2020. Guest editorial: Data science challenges in industry 4.0. IEEE Trans. Ind. Inform. 16 (9), 5924–5928. http://dx.doi.org/10.1109/TII.2020.2984061.

Eriksson, K.M., Olsson, A.K., Carlsson, L., 2024. Beyond lean production practices and industry 4.0 technologies toward the human-centric industry 5.0. Technol. Sustain..

Fantozzi, I.C., Santolamazza, A., Loy, G., Schiraldi, M.M., 2025. Digital twins: Strategic guide to utilize digital twins to improve operational efficiency in industry 4.0. Future Internet 17 (1), http://dx.doi.org/10.3390/fi17010041, URL https://www.mdpi.com/1999-5903/17/1/41.

Faubel, L., Schmid, K., Eichelberger, H., 2023. Mlops challenges in industry 4.0. SN Comput. Sci. 4 (6), 828.

Faubel, L., Woudsma, T., Methnani, L., Ghezeljhemeidan, A.G., Buelow, F., Schmid, K., van Driel, W.D., Kloepper, B., Theodorou, A., Nosratinia, M., Bång, M., 2024. A mlops architecture for XAI in industrial applications. In: 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation. ETFA, pp. 1–4. http://dx.doi.org/10.1109/ETFA61755.2024.10711084.

Felser, M., Rentschler, M., Kleineberg, O., 2019. Coexistence standardization of operation technology and information technology. Proc. IEEE 107 (6), 962–976. http://dx.doi.org/10.1109/JPROC.2019.2901314.

Fernández, F., Zverev, M., Garrido, P., Juárez, J., Bilbao, J., Agüero, R., 2021. Even lower latency in IIoT: Evaluation of QUIC in industrial IoT scenarios. Sens. 21 (17).

Ferrer, B., Lastra, J., 2017. An architecture for implementing private local automation clouds built by CPS. In: IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society. IEEE, pp. 5406–5413.

Fielding, R.T., 2000. Architectural Styles and the Design of Network-Based Software Architectures (Publication). University of California, Irvine.

Figueroa-Lorenzo, S., Añorga, J., Arrizabalaga, S., 2020. A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS. ACM Comput. Surv. 53 (2), http://dx.doi.org/10.1145/3381038.

Filkins, B., Wylie, D., Dely, A., 2019. Sans 2019 state of ot/ics cybersecurity survey. SANS Technol. Inst..

Foehr, M., Vollmar, J., Calà, A., Leitão, P., Karnouskos, S., Colombo, A.W., 2017. Engineering of next generation cyber-physical automation system architectures. Multi-Discip. Eng. Cyber-Phys. Prod. Syst. 185–206. http://dx.doi.org/10.1007/978-3-319-56345-9_8.

Fortinet, 2019. A security approach for protecting converged IT and OT. URL https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-a-security-approach-for-protecting-converged-it-and-ot.pdf.

Gahlawat, D., Suhag, S., Rani, U., Madavi, S., 2023. Hybrid deep learning model for IT-OT integration in industry 4.0. In: 2023 Second International Conference on Smart Technologies for Smart Nation. SmartTechCon, pp. 1025–1030. http://dx.doi.org/10.1109/SmartTechCon57526.2023.10391501.

García-Domínguez, A., Marcos-Bárcena, M., Medina-Bulo, I., Prades-Martell, L., 2013. Towards an integrated SOA-based architecture for interoperable and responsive manufacturing systems. Procedia Eng. 63, 123–132. http://dx.doi.org/10.1016/j.proeng.2013.08.268, The Manufacturing Engineering Society International Conference, MESIC 2013, URL https://www.sciencedirect.com/science/article/pii/S1877705813014811.

Garimella, P.K., 2018. IT-OT integration challenges in utilities. In: 2018 IEEE 3rd International Conference on Computing, Communication and Security. ICCCS, pp. 199–204. http://dx.doi.org/10.1109/CCCS.2018.8586807.

Gawanmeh, A., Alomari, A., 2018. Taxonomy analysis of security aspects in cyber physical systems applications. In: 2018 IEEE International Conference on Communications Workshops. ICC Workshops, pp. 1–6. http://dx.doi.org/10.1109/ICCW.2018.8403559.

Gerrikagoitia, J.K., Unamuno, G., Urkia, E., Serna, A., 2019. Digital manufacturing platforms in the industry 4.0 from private and public perspectives. Appl. Sci. 9 (14), http://dx.doi.org/10.3390/app9142934, URL https://www.mdpi.com/2076-3417/9/14/2934.

Ghildiyal, Y., Singh, R., Alkhayyat, A., Gehlot, A., Malik, P., Sharma, R., Akram, S.V., Alkwai, L.M., 2023. An imperative role of 6G communication with perspective of industry 4.0: Challenges and research directions. Sustain. Energy Technol. Assess. 56, 103047.

Giehl, A., Wiedermann, N., 2018. Security verification of third party design files in manufacturing. In: Proceedings of the 2018 10th International Conference on Computer and Automation Engineering. In: ICCAE 2018, Association for Computing Machinery, New York, NY, USA, pp. 166–173. http://dx.doi.org/10.1145/3192975.3192984.

Gilani, S.S., Jungbluth, F., Flatt, H., Wendt, V., Jasperneite, J., 2016. Alternative controls for soft real-time industrial control services in case of broken cloud links. In: 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation. ETFA, pp. 1–4. http://dx.doi.org/10.1109/ETFA.2016.7733669.

Givehchi, O., Imtiaz, J., Trsek, H., Jasperneite, J., 2014. Control-as-a-service from the cloud: A case study for using virtualized PLCs. In: 2014 10th IEEE Workshop on Factory Communication Systems. WFCS 2014, pp. 1–4. http://dx.doi.org/10.1109/WFCS.2014.6837587.

Givehchi, O., Landsdorf, K., Simoens, P., Colombo, A.W., 2017. Interoperability for industrial cyber-physical systems: An approach for legacy systems. IEEE Trans. Ind. Inform. 13 (6), 3370–3378. http://dx.doi.org/10.1109/TII.2017.2740434.

Grieves, M., 2011. Virtually Perfect: Driving Innovative and Lean Products through Product Lifecycle Management. Space Coast Press.

Grieves, M., Vickers, J., 2016. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In: Transdisciplinary Perspectives on Complex Systems. pp. 85–113. http://dx.doi.org/10.1007/978-3-319-38756-7_4.

Grieves, M., Vickers, J., 2017. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In: Kahlen, F.-J., Flumerfelt, S., Alves, A. (Eds.), Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches. Springer International Publishing, Cham, pp. 85–113.

Grosse, E.H., Sgarbossa, F., Berlin, C., Neumann, W.P., 2023. Human-centric production and logistics system design and management: transitioning from industry 4.0 to industry 5.0. Int. J. Prod. Res. 61 (22), 7749–7759. http://dx.doi.org/10.1080/00207543.2023.2246783.

Group, T.O., The open group standard for SOA reference architecture, visited on December 30, 2024. URL https://www.opengroup.org/soa/source-book/soa_refarch/index.htm.

Gutiérrez, M., Ademaj, A., Steiner, W., Dobrin, R., Punnekkat, S., 2017. Self-configuration of IEEE 802.1 TSN networks. In: 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation. ETFA, pp. 1–8. http://dx.doi.org/10.1109/ETFA.2017.8247597.

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., Banks, M.K., 2020. A review of cybersecurity incidents in the water sector. J. Environ. Eng. 146 (5), 03120003.

Heritage, I., 2019. Protecting industry 4.0: challenges and solutions as IT, OT and IP converge. Netw. Secur. 2019 (10), 6–9. http://dx.doi.org/10.1016/S1353-4858(19)30120-5, URL https://www.sciencedirect.com/science/article/pii/S1353485819301205.

Hicham, T., Khalifa, M., Kamal, E.G., Fatiha, A., 2023. Machine and deep learning applications in industry 4.0. In: 2023 International Conference on Technology, Engineering, and Computing Applications. ICTECA, pp. 1–5. http://dx.doi.org/10.1109/ICTECA60133.2023.10490844.

Hofer, F., 2018. Architecture, technologies and challenges for cyber-physical systems in industry 4.0: A systematic mapping study. In: Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement. ESEM '18, Association for Computing Machinery, New York, NY, USA, http://dx.doi.org/10.1145/3239235.3239242.

Hozdić, E., Kozjek, D., Butala, P., 2020. A cyber-physical approach to the management and control of manufacturing systems. Stroj. Vestnik/J. Mech. Eng. 66 (1).

Huang, S., Wang, B., Li, X., Zheng, P., Mourtzis, D., Wang, L., 2022. Industry 5.0 and society 5.0—Comparison, complementation and co-evolution. J. Manuf. Syst. 64, 424–428. http://dx.doi.org/10.1016/j.jmsy.2022.07.010, URL https://www.sciencedirect.com/science/article/pii/S0278612522001224.

Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., Wang, S., Yu, F.R., Liu, Y., 2022. A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges. IEEE Commun. Surv. Tutor. 24 (1), 88–122. http://dx.doi.org/10.1109/COMST.2022.3141490.

Hupp, W., Hasandka, A., de Carvalho, R.S., Saleem, D., 2020. Module-OT: A hardware security module for operational technology. In: 2020 IEEE Texas Power and Energy Conference. TPEC, pp. 1–6. http://dx.doi.org/10.1109/TPEC48276.2020.9042540.

IEC 61131. URL https://webstore.iec.ch/publication/4552.

2020. IEC 62264-1:2013. URL https://www.iso.org/standard/57308.html.

IIC IIRA.URL https://www.iiconsortium.org/press-room/06-17-15.htm.

Industry 4.0. URL https://www.plattform-i40.de/PI40/Navigation/EN/Home/home.html.

Internet Engineering Task Force (IETF), 2024. Visited on December 30, 2024. [link]. URL https://datatracker.ietf.org/doc/rfc8684/.

Internet of Things (IoT) Bridging the divide: Getting IT, OT to work together for industrial IoT David O'Hara, 2021. Bridging the divide: Getting IT and OT to work together for industrial IoT. URL https://blogs.cisco.com/internet-of-things/bridging-the-divide-getting-it-and-ot-to-work-together-for-industrial-iot.

IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch), visited on December 30, 2024. URL https://datatracker.ietf.org/wg/6tisch/about/.

ISA95, Enterprise-Control System Integration- ISA. URL https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95.

Ivanov, D., 2023. The industry 5.0 framework: viability-based integration of the resilience, sustainability, and human-centricity perspectives. Int. J. Prod. Res. 61 (5), 1683–1695. http://dx.doi.org/10.1080/00207543.2022.2118892.

Iyengar, J., Thomson, M., 2021. QUIC: A UDP-based multiplexed and secure transport. In: RFC 9000. http://dx.doi.org/10.17487/RFC9000, URL https://www.rfc-editor.org/info/rfc9000.

Jamei, M., Stewart, E., Peisert, S., Scaglione, A., McParland, C., Roberts, C., McEachern, A., 2016. Micro synchrophasor-based intrusion detection in automated distribution systems: Toward critical infrastructure security. IEEE Internet Comput. 20 (5), 18–27. http://dx.doi.org/10.1109/MIC.2016.102.

Javaid, M., Haleem, A., Singh, R.P., Rab, S., Suman, R., 2022. Significant applications of cobots in the field of manufacturing. Cogn. Robot. 2, 222–233. http://dx.doi.org/10.1016/j.cogr.2022.10.001, URL https://www.sciencedirect.com/science/article/pii/S2667241322000209.

Jbair, M., Ahmad, B., Ahmad, M.H., Harrison, R., 2018. Industrial cyber physical systems: A survey for control-engineering tools. In: 2018 IEEE Industrial Cyber-Physical Systems. ICPS, pp. 270–276. http://dx.doi.org/10.1109/ICPHYS.2018.8387671.

Jiang, J.-R., 2017. An improved cyber-physical systems architecture for industry 4.0 smart factories. In: 2017 International Conference on Applied System Innovation. ICASI, pp. 918–920. http://dx.doi.org/10.1109/ICASI.2017.7988589.

Jiang, C., Wan, J., 2021. A thing-edge-cloud collaborative computing decision-making method for personalized customization production. IEEE Access 9, 10962–10973. http://dx.doi.org/10.1109/ACCESS.2021.3050238.

Jin, Y., Kulkarni, P., Wilcox, J., Sooriyabandara, M., 2016. A centralized scheduling algorithm for IEEE 802.15.4e TSCH based industrial low power wireless networks. In: 2016 IEEE Wireless Communications and Networking Conference. pp. 1–6. http://dx.doi.org/10.1109/WCNC.2016.7565002.

Kadir, B.A., Broberg, O., Souza da Conceição, C., et al., 2018. Designing human-robot collaborations in industry 4.0: explorative case studies. In: DS 92: Proceedings of the DESIGN 2018 15th International Design Conference. pp. 601–610.

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E.K., Papadourakis, G., 2019. Industrial CyberSecurity 4.0: Preparing the operational technicians for industry 4.0. In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks. CAMAD, pp. 1–6. http://dx.doi.org/10.1109/CAMAD.2019.8858454.

Kasinathan, P., Pugazhendhi, R., Elavarasan, R.M., Ramachandaramurthy, V.K., Ramanathan, V., Subramanian, S., Kumar, S., Nandhagopal, K., Raghavan, R.R.V., Rangasamy, S., Devendiran, R., Alsharif, M.H., 2022. Realization of sustainable development goals with disruptive technologies by integrating industry 5.0, society 5.0, smart cities and villages. Sustainability 14 (22), http://dx.doi.org/10.3390/su142215258, URL https://www.mdpi.com/2071-1050/14/22/15258.

Kavakli, E., Buenabad-Chavez, J., Tountopoulos, V., Loucopoulos, P., Sakellariou, R., 2018. Specification of a software architecture for an industry 4.0 environment. In: 2018 Sixth International Conference on Enterprise Systems. ES, pp. 36–43. http://dx.doi.org/10.1109/ES.2018.00013.

Kegyes, T., Süle, Z., Abonyi, J., 2021. The applicability of reinforcement learning methods in the development of industry 4.0 applications. Complexity 2021 (1), 7179374. http://dx.doi.org/10.1155/2021/7179374.

Keller, B., 2019. Digital innovation to drive intelligent utility enterprise. In: 2019 IEEE International Conference on Energy Internet. ICEI, pp. 484–486. http://dx.doi.org/10.1109/ICEI.2019.00091.

Khan, M.N., Ahmad, I., 2025. Harnessing digital twins: Advancing virtual replicas for optimized system performance and sustainable innovation. Babylon. J. Mech. Eng. 2025, 18–33.

Khare, R., Khadem, M., Moorty, S., Methaprayoon, K., Zhu, J., 2011. Patterns and practices for CIM applications. In: 2011 IEEE Power and Energy Society General Meeting. pp. 1–8. http://dx.doi.org/10.1109/PES.2011.6039268.

Khona, C., 2017. Key Attributes of an Intelligent IIoT Edge Platform. White Paper, Xilinx, San Jose, CA, USA.

Koorapati, K., Ramesh, P.K., Veeraswamy, S., 2018. Ontology based resource management for IoT deployed with SDDC. In: 2018 IEEE International Conference on Cloud Computing in Emerging Markets. CCEM, pp. 39–46. http://dx.doi.org/10.1109/CCEM.2018.00015.

Kupzog, F., Veichtlbauer, A., Heinisch, A., von Tüllenburg, F., Langthaler, O., Pache, U., Jung, O., Frank, R., Dorfinger, P., 2020. The impact of virtualisation techniques on power system control networks. Electronics 9 (9), http://dx.doi.org/10.3390/electronics9091433, URL https://www.mdpi.com/2079-9292/9/9/1433.

Langley, A., Riddoch, A., Wilk, A., Vicente, A., Krasic, C., Zhang, D., Yang, F., Kouranov, F., Swett, I., Iyengar, J., Bailey, J., Dorfman, J., Roskind, J., Kulik, J., Westin, P., Tenneti, R., Shade, R., Hamilton, R., Vasiliev, V., Chang, W.-T., Shi, Z., 2017. The QUIC transport protocol: Design and internet-scale deployment. In: Proceedings of the Conference of the ACM Special Interest Group on Data Communication. SIGCOMM '17, Association for Computing Machinery, pp. 183–196.

Leander, B., Čaušević, A., Hansson, H., 2019. Applicability of the IEC 62443 standard in industry 4.0 / IIoT. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES '19, Association for Computing Machinery, New York, NY, USA, http://dx.doi.org/10.1145/3339252.3341481.

Lee, E.A., Seshia, S.A., 2017. Introduction to Embedded Systems: A Cyber-Physical Systems Approach. The MIT Press.

Li, W.D., JÖrn, M., 2013. Cloud Manufacturing: Distributed Computing Technologies for Global and Sustainable Manufacturing. Springer.

Li, C., Mantravadi, S., Møller, C., 2020. AAU open source MES architecture for smart factories – exploiting ISA 95. In: 2020 IEEE 18th International Conference on Industrial Informatics. INDIN, 1, pp. 369–373. http://dx.doi.org/10.1109/INDIN45582.2020.9442130.

Li, X., Wan, J., Dai, H.-N., Imran, M., Xia, M., Celesti, A., 2019. A hybrid computing solution and resource scheduling strategy for edge computing in smart manufacturing. IEEE Trans. Ind. Inform. 15 (7), 4225–4234. http://dx.doi.org/10.1109/TII.2019.2899679.

Li, J.-Q., Yu, F.R., Deng, G., Luo, C., Ming, Z., Yan, Q., 2017. Industrial internet: A survey on the enabling technologies, applications, and challenges. IEEE Commun. Surv. Tutor. 19 (3), 1504–1526. http://dx.doi.org/10.1109/COMST.2017.2691349.

Lilan, L., Yu'an, H., Tao, Y., Zonghui, X., 2007. Research on SOA-based manufacturing grid and service modes. In: Sixth International Conference on Grid and Cooperative Computing. GCC 2007, pp. 608–613. http://dx.doi.org/10.1109/GCC.2007.108.

Lim, I.-H., Lee, S.-J., Park, J.-H., Shin, Y.-H., 2016. IT/OT convergence advanced distribution management system. Trans. Korean Inst. Electr. Eng. 65 (5), 753–759.

Lin, H., Harding, J., 2007. A manufacturing system engineering ontology model on the semantic web for inter-enterprise collaboration. Comput. Ind. 58 (5), 428–437. http://dx.doi.org/10.1016/j.compind.2006.09.015, URL https://www.sciencedirect.com/science/article/pii/S0166361506001837.

Liu, C., Ding, J., Sun, J., 2021. Reinforcement learning based decision making of operational indices in process industry under changing environment. IEEE Trans. Ind. Inform. 17 (4), 2727–2736. http://dx.doi.org/10.1109/TII.2020.3005207.

Liu, L., Guo, F., Zou, Z., Duffy, V.G., 2024. Application, development and future opportunities of collaborative robots (cobots) in manufacturing: A literature review. Int. J. Hum.–Comput. Interact. 40 (4), 915–932. http://dx.doi.org/10.1080/10447318.2022.2041907.

Liu, Y., Kashef, M., Lee, K.B., Benmohamed, L., Candell, R., 2019. Wireless network design for emerging IIoT applications: Reference framework and use cases. Proc. IEEE 107 (6), 1166–1192. http://dx.doi.org/10.1109/JPROC.2019.2905423.

Liu, X., Ospina, J., Konstantinou, C., 2020. Deep reinforcement learning for cybersecurity assessment of wind integrated power systems. IEEE Access 8, 208378–208394. http://dx.doi.org/10.1109/ACCESS.2020.3038769.

LLC, F.M., 2021. Manufacturing without unplanned downtime could become a reality sooner than you think. URL https://www.forbes.com/sites/forbestechcouncil/2021/02/26/manufacturing-without-unplanned-downtime-could-become-a-reality-sooner-than-you-think/.

LLC., F.M., 2022. Unplanned downtime costs more than you think. URL https://www.forbes.com/sites/forbestechcouncil/2022/02/22/unplanned-downtime-costs-more-than-you-think/.

Lo Bello, L., Steiner, W., 2019. A perspective on IEEE time-sensitive networking for industrial communication and automation systems. Proc. IEEE 107 (6), 1094–1120. http://dx.doi.org/10.1109/JPROC.2019.2905334.

Lobur, M., Tkachenko, S., Khnykin, O., 2011. Researching and creation of SCADA system. In: 2011 11th International Conference the Experience of Designing and Application of CAD Systems in Microelectronics. CADSM, pp. 371–372.

Longo, F., Padovano, A., Umbrello, S., 2020. Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future. Appl. Sci. 10 (12), http://dx.doi.org/10.3390/app10124182, URL https://www.mdpi.com/2076-3417/10/12/4182.

Lu, Y., 2017. Industry 4.0: A survey on technologies, applications and open research issues. J. Ind. Inf. Integr. 6, 1–10. http://dx.doi.org/10.1016/j.jii.2017.04.005, URL https://www.sciencedirect.com/science/article/pii/S2452414X17300043.

Lu, H.-P., Weng, C.-I., 2018. Smart manufacturing technology, market maturity analysis and technology roadmap in the computer and electronic product manufacturing industry. Technol. Forecast. Soc. Change 133, 85–94. http://dx.doi.org/10.1016/j.techfore.2018.03.005, URL https://www.sciencedirect.com/science/article/pii/S0040162517311514.

Mamduhi, M.H., Balta, E.C., Rupenyan, A., Lygeros, J., 2022. Information-operation technology integration in industrial cyberphysical systems. Computer 55 (11), 115–118. http://dx.doi.org/10.1109/MC.2022.3198196.

Manner, I.I.A.S., 2019. Industry 4.0 cybersecurity: Challenges & recommendations. The EU Agency Cybersecur..

Manson, S., Anderson, D., 2019. Cybersecurity for protection and control systems: An overview of proven design solutions. IEEE Ind. Appl. Mag. 25 (4), 14–23. http://dx.doi.org/10.1109/MIAS.2018.2875175.

Meliopoulos, A.P.S., Polymeneas, E., Tan, Z., Huang, R., Zhao, D., 2013. Advanced distribution management system. IEEE Trans. Smart Grid 4 (4), 2109–2117. http://dx.doi.org/10.1109/TSG.2013.2261564.

Mena, M., Criado, J., Iribarne, L., Corral, A., 2019. Digital dices: Towards the integration of cyber-physical systems merging the web of things and microservices. In: Model and Data Engineering: 9th International Conference, MEDI 2019, Toulouse, France, October 28–31, 2019, Proceedings. pp. 195–205.

Michailidis, E.T., Potirakis, S.M., Kanatas, A.G., 2020. AI-inspired non-terrestrial networks for IIoT: Review on enabling technologies and applications. IoT 1 (1), 21–48. http://dx.doi.org/10.3390/iot1010003, URL https://www.mdpi.com/2624-831X/1/1/3.

Minet, P., Khoufi, I., Laouiti, A., 2017. Increasing reliability of a TSCH network for the industry 4.0. In: 2017 IEEE 16th International Symposium on Network Computing and Applications. NCA, pp. 1–10. http://dx.doi.org/10.1109/NCA.2017.8171344.

Minoli, D., Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet Things 1–2, 1–13. http://dx.doi.org/10.1016/j.iot.2018.05.002, URL https://www.sciencedirect.com/science/article/pii/S2542660518300167.

Modoni, G.E., Sacco, M., 2023. A human digital-twin-based framework driving human centricity towards industry 5.0. Sensors 23 (13), http://dx.doi.org/10.3390/s23136054, URL https://www.mdpi.com/1424-8220/23/13/6054.

Moghaddam, M., Cadavid, M.N., Kenley, C.R., Deshmukh, A.V., 2018. Reference architectures for smart manufacturing: A critical review. J. Manuf. Syst. 49, 215–225. http://dx.doi.org/10.1016/j.jmsy.2018.10.006, URL https://www.sciencedirect.com/science/article/pii/S0278612518301043.

Montori, F., Zyrianoff, I., Gigli, L., Calvio, A., Venanzi, R., Sindaco, S., Sciullo, L., Zonzini, F., Zauli, M., Testoni, N., Bertacchini, A., Londero, E., Alessi, E., Felice, M.D., Bononi, L., Bellavista, P., De Marchi, L., Marzani, A., Azzoni, P., Cinotti, T.S., 2023. An IoT toolchain architecture for planning, running and managing a complete condition monitoring scenario. IEEE Access 11, 6837–6856. http://dx.doi.org/10.1109/ACCESS.2023.3237971.

Montori, F., Zyrianoff, I., Gigli, L., Venanzi, R., Sindaco, S., Aguzzi, C., Zonzini, F., Zauli, M., Testoni, N., Alessi, E., Felice, M.D., Bononi, L., Bellavista, P., De Marchi, L., Cinotti, T.S., 2021. A toolchain architecture for condition monitoring using the eclipse arrowhead framework. In: IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society. pp. 1–6. http://dx.doi.org/10.1109/IECON48115.2021.9589532.

Moraes, A., Carvalho, A.M., Sampaio, P., 2023. Lean and industry 4.0: a review of the relationship, its limitations, and the path ahead with industry 5.0. Machines 11 (4), 443.

Morariu, C., Borangiu, T., 2012. Manufacturing integration framework: A SOA perspective on manufacturing. IFAC Proc. Vol. 45 (6), 31–38. http://dx.doi.org/10.3182/20120523-3-RO-2023.00445, URL https://www.sciencedirect.com/science/article/pii/S1474667016331226, 14th IFAC Symposium on Information Control Problems in Manufacturing.

Morawski, M., Ignaciuk, P., 2021. A green multipath TCP framework for industrial internet of things applications. Comput. Netw. 187, 107831. http://dx.doi.org/10.1016/j.comnet.2021.107831.

Moufaddal, M., Benghabrit, A., Bouhaddou, I., 2019. Industry 4.0: A roadmap to digital supply chains. In: 2019 1st International Conference on Smart Systems and Data Science. ICSSD, pp. 1–9. http://dx.doi.org/10.1109/ICSSD47982.2019.9002751.

Mourtzis, D., Angelopoulos, J., Panopoulos, N., 2022. A literature review of the challenges and opportunities of the transition from industry 4.0 to society 5.0. Energies 15 (17), http://dx.doi.org/10.3390/en15176276, URL https://www.mdpi.com/1996-1073/15/17/6276.

Mqtt, MQTT, The Standard for IoT Messaging, visited on December 30, 2024. URL https://mqtt.org/.

Murray, G., Johnstone, M.N., Valli, C., 2017. The convergence of IT and OT in critical infrastructure. Aust. Inf. Secur. Manag. Conf..

Nahavandi, S., 2019. Industry 5.0—A human-centric solution. Sustain. 11 (16), http://dx.doi.org/10.3390/su11164371, URL https://www.mdpi.com/2071-1050/11/16/4371.

Nair, M.M., Tyagi, A.K., Sreenath, N., 2021. The future with industry 4.0 at the core of society 5.0: Open issues, future opportunities and challenges. In: 2021 International Conference on Computer Communication and Informatics. ICCCI, pp. 1–7. http://dx.doi.org/10.1109/ICCCI50826.2021.9402498.

Negri, E., Fumagalli, L., Macchi, M., 2017. A review of the roles of digital twin in CPS-based production systems. Procedia Manuf. 11, 939–948. http://dx.doi.org/10.1016/j.promfg.2017.07.198, URL https://www.sciencedirect.com/science/article/pii/S2351978917304067, 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy.

Nguyen-Hoang, P., Vo-Tan, P., 2019. Development an open-source industrial IoT gateway. In: 2019 19th International Symposium on Communications and Information Technologies. ISCIT, pp. 201–204. http://dx.doi.org/10.1109/ISCIT.2019.8905157.

Nian, R., Liu, J., Huang, B., 2020. A review on reinforcement learning: Introduction and applications in industrial process control. Comput. Chem. Eng. 139, 106886.

Niknejad, N., Ismail, W., Ghani, I., Nazari, B., Bahari, M., et al., 2020. Understanding service-oriented architecture (SOA): A systematic literature review and directions for further investigation. Inf. Syst. 91, 101491.

Niu, S., Kong, W., Chen, L., Zhou, X., Wang, N., 2025. Privacy-preserving and verifiable federated learning with weighted average aggregation in edge computing. J. Netw. Comput. Appl. 240, 104201. http://dx.doi.org/10.1016/j.jnca.2025.104201, URL https://www.sciencedirect.com/science/article/pii/S1084804525000980.

Nuaimi, M., Fourati, L.C., Hamed, B.B., 2023. Intelligent approaches toward intrusion detection systems for industrial Internet of Things: A systematic comprehensive review. J. Netw. Comput. Appl. 215, 103637. http://dx.doi.org/10.1016/j.jnca.2023.103637, URL https://www.sciencedirect.com/science/article/pii/S1084804523000565.

The openplc project. URL http://www.openplcproject.com/.

Oztemel, E., Gursev, S., 2018. Literature review of Industry 4.0 and related technologies. J. Intell. Manuf. 31 (1), 127–182. http://dx.doi.org/10.1007/s10845-018-1433-8.

Paes, R., Mazur, D.C., Venne, B.K., Ostrzenski, J., 2020. A guide to securing industrial control networks: Integrating IT and OT systems. IEEE Ind. Appl. Mag. 26 (2), 47–53. http://dx.doi.org/10.1109/MIAS.2019.2943630.

Pariyani, A., Bespalov, D., Oktem, U.G., Cielak, L., 2016. Dynamic prediction of risk levels for manufacturing operations through leading risk indicators: dynamic risk analyzer engine.

Park, H.M., Wook Jeon, J., 2019. OPC UA based universal edge gateway for legacy equipment. In: 2019 IEEE 17th International Conference on Industrial Informatics. INDIN, vol. 1, pp. 1002–1007. http://dx.doi.org/10.1109/INDIN41052.2019.8972187.

Pei, Q., Yu, F.R., Ota, K., Atiquzzaman, M., Lu, Y., 2025. Next-generation web 3.0 for digitalized industrial applications in the 5G/6G era. Future Gener. Comput. Syst. 173, 107835. http://dx.doi.org/10.1016/j.future.2025.107835, URL https://www.sciencedirect.com/science/article/pii/S0167739X2500130X.

Pettorali, M., Righetti, F., Vallati, C., Das, S.K., Anastasi, G., 2024. Mobility management in TSCH-based industrial wireless networks. IEEE Trans. Mob. Comput. 23 (9), 8710–8728. http://dx.doi.org/10.1109/TMC.2024.3354798.

Pittalà, G.F., Rinieri, L., Al Sadi, A., Davoli, G., Melis, A., Prandini, M., Cerroni, W., 2024. Leveraging data plane programmability to enhance service orchestration at the edge: A focus on industrial security. Comput. Netw. 246, 110397. http://dx.doi.org/10.1016/j.comnet.2024.110397, URL https://www.sciencedirect.com/science/article/pii/S1389128624002299.

Pokhrel, S.R., Garg, S., 2021. Multipath communication with deep Q-network for industry 4.0 automation and orchestration. IEEE Trans. Ind. Inform. 17 (4), 2852–2859. http://dx.doi.org/10.1109/TII.2020.3000502.

Pokhrel, S.R., Pan, L., Kumar, N., Doss, R., Vu, H.L., 2021. Multipath TCP meets transfer learning: A novel edge-based learning for industrial IoT. IEEE Internet Things J. 8 (13), 10299–10307.

Pop, P., Raagaard, M.L., Gutierrez, M., Steiner, W., 2018. Enabling fog computing for industrial automation through time-sensitive networking (TSN). IEEE Commun. Stand. Mag. 2 (2), 55–61. http://dx.doi.org/10.1109/MCOMSTD.2018.1700057.

Pop, P., Zarrin, B., Barzegaran, M., Schulte, S., Punnekkat, S., Ruh, J., Steiner, W., 2021. The FORA fog computing platform for industrial IoT. Inf. Syst. 98, 101727. http://dx.doi.org/10.1016/j.is.2021.101727, URL https://www.sciencedirect.com/science/article/pii/S0306437921000053.

Prinsloo, J., Sinha, S., von Solms, B., 2019. A review of industry 4.0 manufacturing process security risks. Appl. Sci. 9 (23), http://dx.doi.org/10.3390/app9235105, URL https://www.mdpi.com/2076-3417/9/23/5105.

Qi, Q., Tao, F., 2018. Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison. IEEE Access 6, 3585–3593. http://dx.doi.org/10.1109/ACCESS.2018.2793265.

Qi, Q., Tao, F., 2019. A smart manufacturing service system based on edge computing, fog computing, and cloud computing. IEEE Access 7, 86769–86777. http://dx.doi.org/10.1109/ACCESS.2019.2923610.

Queiroz, R., Cruz, T., Mendes, J., Sousa, P., Simões, P., 2023. Container-based virtualization for real-time industrial systems—a systematic review. ACM Comput. Surv. 56 (3), 1–38.

Rahardjo, B., Wang, F.-K., Lo, S.-C., Chu, T.-H., 2024. A sustainable innovation framework based on lean six sigma and industry 5.0. Arab. J. Sci. Eng. 49 (5), 7625–7642.

Rajkumar, R., Lee, I., Sha, L., Stankovic, J., 2010. Cyber-physical systems: The next computing revolution. In: Design Automation Conference. pp. 731–736. http://dx.doi.org/10.1145/1837274.1837461.

Ram Kumar, R., Menon, S., Nair, N.S., 2020. Blockchain solutions for security threats in smart industries. In: 2020 Fourth International Conference on Computing Methodologies and Communication. ICCMC, pp. 756–763. http://dx.doi.org/10.1109/ICCMC48092.2020.ICCMC-000141.

RAMI 4.0 - ISA. URL https://www.isa.org/intech-home/2019/march-april/features/rami-4-0-reference-architectural-model-for-industr.

Rannertshauser, P., Kessler, M., Arlinghaus, J.C., 2022. Human-centricity in the design of production planning and control systems: A first approach towards industry 5.0. IFAC-PapersOnLine 55 (10), 2641–2646. http://dx.doi.org/10.1016/j.ifacol.2022.10.108, URL https://www.sciencedirect.com/science/article/pii/S2405896322021176. 10th IFAC Conference on Manufacturing Modelling, Management and Control MIM 2022.

Rao, S.K., Prasad, R., 2018. Impact of 5G technologies on industry 4.0. Wirel. Pers. Commun. 100, 145–159.

Raptis, T.P., Passarella, A., Conti, M., 2019. Data management in industry 4.0: State of the art and open challenges. IEEE Access 7, 97052–97093. http://dx.doi.org/10.1109/ACCESS.2019.2929296.

Ren, J., Ahmad, R., Li, D., Ma, Y., Hui, J., 2025. Industrial applications of digital twins: A systematic investigation based on bibliometric analysis. Adv. Eng. Inform. 65, 103264. http://dx.doi.org/10.1016/j.aei.2025.103264, URL https://www.sciencedirect.com/science/article/pii/S1474034625001570.

Rosa, L., Freitas, M., Mazo, S., Monteiro, E., Cruz, T., Simões, P., 2019. A comprehensive security analysis of a SCADA protocol: From OSINT to mitigation. IEEE Access 7, 42156–42168. http://dx.doi.org/10.1109/ACCESS.2019.2906926.

Sadi, A.A., Savi, M., Melis, A., Prandini, M., Callegati, F., 2024. Unleashing dynamic pipeline reconfiguration of P4 switches for efficient network monitoring. IEEE Trans. Netw. Serv. Manag. 21 (3), 3482–3497. http://dx.doi.org/10.1109/TNSM.2024.3377538.

Sahan, A.M., Kathiravan, S., Lokesh, M., Raffik, R., 2023. Role of cobots over industrial robots in industry 5.0: A review. In: 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation. ICAECA, pp. 1–5. http://dx.doi.org/10.1109/ICAECA56562.2023.10201199.

Sajitha, P., Andrushia, A.D., Anand, N., Naser, M., 2024. A review on machine learning and deep learning image-based plant disease classification for industrial farming systems. J. Ind. Inf. Integr. 38, 100572. http://dx.doi.org/10.1016/j.jii.2024.100572.

Sajjadi, M., Niknia, B., 2013. Smart power grid security services: Risk management approach considering both OT and it domains case study: Shiraz power distribution company. In: 22nd International Conference and Exhibition on Electricity Distribution. CIRED 2013, pp. 1–4. http://dx.doi.org/10.1049/cp.2013.1099.

Samitier, C., 2017. Utility Communication Networks and Services Specification, Deployment and Operation. Springer International Publishing.

Sampath Kumar, V.R., Khamis, A., Fiorini, S., Carbonera, J.L., Olivares Alarcos, A., Habib, M., Goncalves, P., Li, H., Olszewska, J.I., 2019. Ontologies for industry 4.0. Knowl. Eng. Rev. 34, e17. http://dx.doi.org/10.1017/S0269888919000109.

Sandberg, C., Hunter, B., 2017. Cyber security primer for legacy process plant operation. In: 2017 Petroleum and Chemical Industry Technical Conference. PCIC, pp. 97–102. http://dx.doi.org/10.1109/PCICON.2017.8188728.

Schevers, H., Drogemuller, R., 2005. Converting the industry foundation classes to the web ontology language. In: 2005 First International Conference on Semantics, Knowledge and Grid. http://dx.doi.org/10.1109/SKG.2005.59, 73–73.

Sciullo, L., Bhattacharjee, S., Kovatsch, M., 2020. Bringing deterministic industrial networking to the W3C web of things with TSN and OPC UA. In: Proceedings of the 10th International Conference on the Internet of Things. IoT '20, Association for Computing Machinery, New York, NY, USA, http://dx.doi.org/10.1145/3410992.3410997.

Shi, J., Wan, J., Yan, H., Suo, H., 2011. A survey of cyber-physical systems. In: 2011 International Conference on Wireless Communications and Signal Processing. WCSP, pp. 1–6. http://dx.doi.org/10.1109/WCSP.2011.6096958.

Shrestha, B., Lin, H., 2020. Data-centric edge computing to defend power grids against IoT-based attacks. Computer 53 (5), 35–43. http://dx.doi.org/10.1109/MC.2020.2972228.

Šindelář, R., Novák, P., 2012. Simulation integration framework. In: IEEE 10th International Conference on Industrial Informatics. pp. 80–85. http://dx.doi.org/10.1109/INDIN.2012.6301221.

Singh, S., Shehab, E., Higgins, N., Fowler, K., Tomiyama, T., Fowler, C., 2018. Challenges of digital twin in high value manufacturing. In: Aerospace Systems and Technology Conference. SAE International, http://dx.doi.org/10.4271/2018-01-1928.

Siqueira, F., Davis, J.G., Service computing for industry 4.0: State of the art, challenges, and research opportunities. 54 (9).

Souvent, A., Kodek, T., Suljanović, N., 2019. CIM-based integration in smart grids: Slovenian use cases. In: 2019 18th International Symposium INFOTEH-JAHORINA. INFOTEH, pp. 1–6. http://dx.doi.org/10.1109/INFOTEH.2019.8717776.

Souza, R., Ferenhof, H., Forcellini, F., 2022. Industry 4.0 and industry 5.0 from the lean perspective. Int. J. Manag. Knowl. Learn. 11.

Standard, I.D., 2020a. IEEE draft standard for information technology– Telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 1: Enhancements for high efficiency WLAN. In: IEEE P802.11ax/D8.0, October 2020. pp. 1–820.

Standard, I.D., 2020b. IEEE draft standard for information technology-telecommunications and information exchange between systems - Local and metropolitan area networks-specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications-amendment 2: Enhanced throughput for operation in license-exempt bands above 45 GHz. In: IEEE P802.11ay/D7.0, December 2020. pp. 1–784.

Std, I., 2020. IEEE standard for low-rate wireless networks. In: IEEE Std 802.15.4-2020 (Revision IEEE Std 802.15.4-2015). pp. 1–800. http://dx.doi.org/10.1109/IEEESTD.2020.9144691.

Stracener, C., Samelson, Q., Mackie, J., Ihaza, M., 2019. The internet of things grows artificial intelligence and data sciences. IT Prof. 21 (3), 55–62. http://dx.doi.org/10.1109/MITP.2019.2912729.

Stratogiannis, D.G., Gkiala-Fikari, S., 2018. Smart grid architecture, communications and data model: The WiseGRID approach. In: 2018 Global Information Infrastructure and Networking Symposium. GIIS, pp. 1–5. http://dx.doi.org/10.1109/GIIS.2018.8635708.

Tabouche, A., Djamaa, B., Senouci, M.R., 2023. Traffic-aware reliable scheduling in TSCH networks for industry 4.0: A systematic mapping review. IEEE Commun. Surv. Tutor. 25 (4), 2834–2861. http://dx.doi.org/10.1109/COMST.2023.3302157.

Tao, F., Cheng, Y., Xu, L.D., Zhang, L., Li, B.H., 2014. CCIoT-CMfg: Cloud computing and internet of things-based cloud manufacturing service system. IEEE Trans. Ind. Inform. 10 (2), 1435–1442. http://dx.doi.org/10.1109/TII.2014.2306383.

Tao, F., Qi, Q., Liu, A., Kusiak, A., 2018. Data-driven smart manufacturing. J. Manuf. Syst. 48, 157–169. http://dx.doi.org/10.1016/j.jmsy.2018.01.006, Special Issue on Smart Manufacturing, URL https://www.sciencedirect.com/science/article/pii/S0278612518300062.

Tasci, T., Melcher, J., Verl, A., 2018. A container-based architecture for real-time control applications. In: 2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings. IEEE, pp. 1–9. http://dx.doi.org/10.1109/ICE.2018.8436369.

Tazzioli, D., Venanzi, R., Capponi, A., Dost, S., Foschini, L., Bellavista, P., 2023. AWS IoT service integration for real industry 4.0 deployments. In: GLOBECOM 2023-2023 IEEE Global Communications Conference. IEEE, pp. 2620–2625.

Tazzioli, D., Venanzi, R., Foschini, L., 2024. Stateful service migration support for kubernetes-based orchestration in industry 4.0. In: 2024 IEEE Symposium on Computers and Communications. ISCC, pp. 1–6. http://dx.doi.org/10.1109/ISCC61673.2024.10733711.

Teles Hermeto, R., Gallais, A., Theoleyre, F., 2017. Scheduling for IEEE802.15.4-TSCH and slow channel hopping MAC in low power industrial wireless networks: A survey. Comput. Commun. 114, 84–105.

Thames, L., Schaefer, D., 2016. Software-defined cloud manufacturing for industry 4.0. Procedia CIRP 52, 12–17. http://dx.doi.org/10.1016/j.procir.2016.07.041, URL https://www.sciencedirect.com/science/article/pii/S2212827116307910, The Sixth International Conference on Changeable, Agile, Reconfigurable and Virtual Production (CARV2016).

Time-Sensitive Networking (TSN) Task Group, 2020. Visited on December 30 2024, URL https://1.ieee802.org/tsn/.

Trotta, D., Garengo, P., 2019. Assessing industry 4.0 maturity: An essential scale for SMEs. In: 2019 8th International Conference on Industrial Technology and Management. ICITM, pp. 69–74. http://dx.doi.org/10.1109/ICITM.2019.8710716.

Ujvarosi, A., 2016. Evolution of SCADA systems. Bull. Transilv. Univ. Brasov. Eng. Sci. Ser. I 9 (1), 63.

2019. Unified architecture. URL https://opcfoundation.org/about/opc-technologies/opc-ua/.

Venanzi, R., Cavalucci, A., Foschini, L., Bellavista, P., 2021. MIINT: Middleware for IIoT platforms integration. In: 2021 IEEE Global Communications Conference. GLOBECOM, pp. 1–6. http://dx.doi.org/10.1109/GLOBECOM46510.2021.9685653.

Venanzi, R., Dahdal, S., Solimando, M., Campioni, L., Cavalucci, A., Govoni, M., Tortonesi, M., Foschini, L., Attana, L., Tellarini, M., Stefanelli, C., 2023a. Enabling adaptive analytics at the edge with the bi-rex big data platform. Comput. Ind. 147, http://dx.doi.org/10.1016/j.compind.2023.103876, URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149292691&doi=10.1016%2fj.compind.2023.103876&partnerID=40&md5=d6ccf776da88d09f45170a28d089a970.

Venanzi, R., Montori, F., Bellavista, P., Foschini, L., 2020. Industry 4.0 solutions for interoperability: a use case about tools and tool chains in the arrowhead tools project. In: 2020 IEEE International Conference on Smart Computing. SMARTCOMP, pp. 429–433. http://dx.doi.org/10.1109/SMARTCOMP50058.2020.00089.

Venanzi, R., Solimando, M., Patrali, M., Foschini, L., Chatzimisios, P., 2023b. Siemens and edgex IIoT platforms: A functional and performance evaluation. In: ICC 2023-IEEE International Conference on Communications. IEEE, pp. 834–839.

Vilajosana, X., Watteyne, T., Chang, T., Vučinić, M., Duquennoy, S., Thubert, P., 2020. IETF 6TiSCH: A tutorial. IEEE Commun. Surv. Tutor. 22 (1), 595–615. http://dx.doi.org/10.1109/COMST.2019.2939407.

Weiss, A., Wortmeier, A.-K., Kubicek, B., 2021. Cobots in industry 4.0: A roadmap for future practice studies on human–robot collaboration. IEEE Trans. Hum.-Mach. Syst. 51 (4), 335–345. http://dx.doi.org/10.1109/THMS.2021.3092684.

When IT and Operational Technology Converge. URL https://www.gartner.com/smarterwithgartner/when-it-and-operational-technology-converge/.

Wortmann, A., Combemale, B., Barais, O., 2017. A systematic mapping study on modeling for industry 4.0. In: Proceedings of the ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems. MODELS '17, IEEE Press, pp. 281–291. http://dx.doi.org/10.1109/MODELS.2017.14.

Wu, H., Alay, Ö., Brunstrom, A., Ferlin, S., Caso, G., 2020. Peekaboo: Learning-based multipath scheduling for dynamic heterogeneous environments. IEEE J. Sel. Areas Commun. 38 (10), 2295–2310.

Wübbeke, J., Meissner, M., Zenglein, M.J., Ives, J., Conrad, B., 2017. MADE IN CHINA 2025 the making of a high-tech superpower and its implications for industrial countries. Handout Hambg. Summit URL http://www.cittc.it/wp-content/uploads/2017/07/MERICS-Made-in-China-2025.pdf.

Xu, X., Lu, Y., Vogel-Heuser, B., Wang, L., 2021. Industry 4.0 and industry 5.0—Inception, conception and perception. J. Manuf. Syst. 61, 530–535. http://dx.doi.org/10.1016/j.jmsy.2021.10.006, URL https://www.sciencedirect.com/science/article/pii/S0278612521002119.

Xu, Z., Tang, J., Yin, C., Wang, Y., Xue, G., 2019. Experience-driven congestion control: When multi-path TCP meets deep reinforcement learning. IEEE J. Sel. Areas Commun. 37 (6), 1325–1336.

Xu, H., Yu, W., Griffith, D., Golmie, N., 2018. A survey on industrial internet of things: A cyber-physical systems perspective. IEEE Access 6, 78238–78259. http://dx.doi.org/10.1109/ACCESS.2018.2884906.

Yang, L., Li, M., Zhang, Y., Si, P., Wang, Z., Yang, R., 2020. Resource management for energy-efficient and blockchain-enabled industrial IoT: A DRL approach. In: 2020 IEEE 6th International Conference on Computer and Communications. ICCC, pp. 910–915. http://dx.doi.org/10.1109/ICCC51575.2020.9345166.

Yannuzzi, M., Irons-Mclean, R., van Lingen, F., Raghav, S., Somaraju, A., Byers, C., Zhang, T., Jain, A., Curado, J., Carrera, D., Trullols, O., Alonso, S., 2017. Toward a converged OpenFog and ETSI MANO architecture. In: 2017 IEEE Fog World Congress. FWC, pp. 1–6. http://dx.doi.org/10.1109/FWC.2017.8368535.

Yi, M., Mueller, H., Yu, L., Chuan, J., 2017. Benchmarking cloud-based SCADA system. In: 2017 IEEE International Conference on Cloud Computing Technology and Science. CloudCom, pp. 122–129. http://dx.doi.org/10.1109/CloudCom.2017.25.

Yonemura, K., Sato, J., Komura, R., Matsuoka, M., 2018. Practical security education on combination of OT and ICT using gamfication method. In: 2018 IEEE Global Engineering Education Conference. EDUCON, pp. 746–750. http://dx.doi.org/10.1109/EDUCON.2018.8363305.

Zawra, L.M., Mansour, H.A., Messiha, N.W., 2019. Migration of legacy industrial automation systems in the context of industry 4.0- a comparative study. In: 2019 International Conference on Fourth Industrial Revolution. ICFIR, pp. 1–7. http://dx.doi.org/10.1109/ICFIR.2019.8894776.

Zhang, S., 2019. Apply SOA paradigms in cyber-physical system to enhance interoperability: State-of-the-art review. arXiv:1903.00065.