

# Real-Time Performance of Industrial IoT Communication Technologies: A Review

Ilja Behnke\*, Henrik Austad†

\*Technische Universität Berlin, Berlin. *i.behnke@tu-berlin.de*

†SINTEF Digital, Trondheim. *henrik.austad@sintef.no*

arXiv:2311.08852v1 [cs.NI] 15 Nov 2023

**Abstract**—With the growing need for automation and the ongoing merge of OT and IT, industrial networks have to transport a high amount of heterogeneous data with mixed criticality such as control traffic, sensor data, and configuration messages. Current advances in IT technologies furthermore enable a new set of automation scenarios under the roof of Industry 4.0 and IIoT where industrial networks now have to meet new requirements in flexibility and reliability. The necessary real-time guarantees will place significant demands on the networks. In this paper, we identify IIoT use cases and infer real-time requirements along several axes before bridging the gap between real-time network technologies and the identified scenarios. We review real-time networking technologies and present peer-reviewed works from the past 5 years for industrial environments. We investigate how these can be applied to controllers, systems, and embedded devices. Finally, we discuss open challenges for real-time communication technologies to enable the identified scenarios. The review shows academic interest in the field of real-time communication technologies but also highlights a lack of a fixed set of standards important for trust in safety and reliability, especially where wireless technologies are concerned.

**Index Terms**—real-time, networks, IIoT, CPS, Industry 4.0

## I. INTRODUCTION

Science and technology are bridging the mechanized industry with the digital world to automate as many processes as possible by connecting operational technologies and business networks. Such a pervasive sensor integration combined with a high degree of network interconnectedness, both between operational technologies (OT), and between OT and "back office" systems (IT), is often described as "IT/OT convergence". It is also known as "Industry 4.0". Examples of envisioned Industry 4.0 scenarios are autonomous drones [1], remote control [2], real-time monitoring [3], and predictive maintenance [4].

In a recent study [5] regarding the usage of pervasive Industrial Internet of Things (IIoT) sensor data, a large majority of the respondents expect Industry 4.0 to provide agility to scale the production to match demands, improved flexibility to customize products, and a reduced time to market for new products. The same participants reported that the current usage of IoT sensors in their systems was primarily used for remote monitoring of equipment, asset and material tracking, and predictive maintenance. Hence, to fully realize the potential of Industry 4.0, pervasive sensor coverage and interconnectedness are essential. To achieve this, great demands will be placed on the networks used in industrial systems. What used to work for Operation Technology (OT) systems will require a much higher degree of flexibility and scalability than what has been available in the past.

Furthermore, advancements in Cyber-Physical Systems (CPSs) increase the real-time requirements for industrial networks. CPSs combine embedded systems with cybernetic control systems to control the physical world from the networked space. The physical processes involved often place strict real-time requirements on CPSs. Command, control, and safety considerations of different criticality levels demand constant latency and predictability, often implemented on small and restricted embedded systems. By attaching these embedded systems to larger networks and incorporating them into complex distributed systems, the same real-time requirements are extended to the network and its participants. Use cases with time-critical control tasks are spread over a network, requiring predictable and reliable packet routing through it.

However, networking concepts like the Internet Protocol (IP) and packet routing are not created to consider real-time demands. IP networks work on a best-effort basis. Packets are indiscriminately routed over a variable number of networking devices, with very limited predictability concerning latency and arrival. The jitter introduced by wireless communication complicates a number of envisioned scenarios including mobile devices.

To meet the real-time demands of networking introduced by envisioned IIoT scenarios, established specialized protocols and standards exist. At the same time, current works in research attend to IIoT-specific requirements such as scalability [6], integration of business and factory networks [7], and mobile computing [8].

In this article, we present and discuss existing standards and technologies as well as present recent works concerning real-time IIoT networking solutions. To this end, we

- identify and present current IIoT scenarios attended to in research,
- derive their real-time networking requirements,
- review established real-time networking technologies,
- presents the most notable recent research,
- and discuss open challenges.

The remainder of this article is structured as follows. Section II identifies IIoT scenario classes and derives real-time networking requirements. Section III reviews the path of networking in industrial systems and presents existing standards designed for industrial networks. Section IV presents ongoing academic works on real-time networking. Section V discusses the feasibility of existing and ongoing solutions. Section VI presents related industrial networking surveys. Section VII concludes this article.

## II. REGARDED IIOT SCENARIOS

In this section, we perform a preliminary literature survey to identify IIoT scenarios containing real-time and network requirements. To this end, we classify the scenarios into groups as depicted in Table I. Network and real-time requirements are derived from the scenario groups to prepare the following survey on enabling technology standards and recent works. A total of 31 research papers with IIoT scenarios of interest have been reviewed. The papers and articles chosen were peer-reviewed and published in the past 10 years. The extracted use cases were either the main focus of a paper or example implementations for evaluation purposes.

Using the identified scenario classes, we hope to get a better understanding of network requirements concerning predictability, latency, and bandwidth. These requirements will then be used in the following sections to assess proposed IIoT real-time networking solutions. Furthermore, we identify relevant network components for each scenario class.

### A. Scenario Classes

*a) Autonomous Vehicles & Automation:* Warehouses and manufacturing sites are getting under pressure to fulfill an ever-increasing demand. To this end, conventional rigid automation is being exchanged for more flexible autonomous solutions controlled via IoT-connected sensors [11]. Autonomously moving machines such as transport robots, forklifts, and warehouse robots pose challenges yet to be solved, especially when employed at a large scale or in close proximity to human workers. Autonomous vehicles have to navigate through dynamic environments making decisions for real-time controlled electric motors [13] while being dependent on communication networks to prevent collisions and improve efficiency [10, 12].

Converging these real-time and networking requirements still requires research, especially considering the necessity for wireless communication. Since moving, potentially dangerous machines are involved, predictability and latency requirements are high. Bandwidth requirements are implementation-specific, with the main factor being whether high-volume sensor data (e.g. video, LIDAR) is transmitted for analysis.

*b) Remote Control:* Industrial Control Systems (ICS) can be changed to make use of the IIoT paradigm by physically shifting controlling entities away from the real-time device, possibly outside of the plant floor [18]. To this end, the originally existing air gap between ICS and external networks has to be bridged [15]. Besides the resulting security implications, this also means opening up real-time control systems to conventional IP networks and protocols. Use-cases furthermore include the remote control of vehicles in inaccessible places [14].

Again, real-time requirements are to be considered as high, since we are regarding moving machines. Some use cases furthermore need wireless communication technologies to work. Bandwidth requirements are low as only control commands need to be transmitted.

*c) Data Analysis & Monitoring:* With the help of sensors on factory floors, a high amount of real-time data can be used to improve business automation, monitoring, and decision-making. To this end, potentially broad data streams have to be transmitted sharing a medium with real-time control traffic [20]. Use cases include data aggregation by wireless sensor networks [21] and predictive maintenance on IIoT sensor data [19]. IT/OT integration also plays a role in monitoring and data analysis. Real-time information from IIoT sensors can help make business decisions and enable automating certain use-cases such as active energy management [7].

This scenario class, while somewhat dependent on real-time data streams does not contain hard real-time tasks. Hence requirements in this regard are negligible. However, due to the large amount of collective data produced by the high number of sensors, bandwidth requirements are usually high. With data-intensive applications benefitting from offloading, bandwidth requirements can be considered high for many use cases.

*d) Worker Safety & Hazard Protection:* Most considered works regard the introduction of IIoT to safety critical systems as a relevant risk factor. Safety in this case means the physical protection of workers and equipment. Due to the attack vector granted by the new connectivity, safety is more conjoined with security than ever [23]. Yet, some works promote the use of interconnected devices for better safety in high-risk environments such as in the mining industry. IIoT technologies can be used to monitor access to hazardous areas around operating machinery, improve documentation/monitoring of maintenance that requires shutdown of the machinery, and prevent unexpected startup or movement during machine maintenance activities [24–26].

Safety solutions distinguish between informational and automatizing setups. Purely informational scenarios react to real-time sensor data by issuing alarms or notifying workers and human operators. Smart monitoring and data analysis in the cloud make these scenarios and their real-time requirements similar to the *Data Analysis* class. Systems that automatically react to hazards such as fire, toxic gases, or dangerous proximity require the highest predictability and latency. However, reactive systems should work independently, making distributed solutions unsuitable.

*e) Task Offloading:* IIoT devices, like traditional embedded systems, only have limited computing capabilities due to power and space constraints. To this end, current research, especially in the field of mobile edge computing, considers the offloading of delay-sensitive tasks to local servers. The main challenges are the guarantee of maximum delays over shared networking channels and compute resources [29]. Subject to offloading is mostly soft real-time tasks for better Quality of Service (QoS) where a balance between latency and reliability has to be found [31].

Due to the nature of offloading, hard real-time tasks with high requirements in predictability are not considered. At the same time, while offloading to more powerful machines can reduce computation time, latency requirements that are too tight to accommodate network delays cannot be accommodated.

TABLE I  
IIOT SCENARIO CLASSES

Scenario Class	References	Predictability Requirement	Latency Requirement	Bandwidth Requirement	Wireless Communication
I Autonomous Vehicles & Mobile Robots	[1, 9–13]	high	medium	variable	essential
II Remote Control of Machines	[14–18]	high	high	low	not necessary
III Sensor Data Analysis & Monitoring	[7, 19–22]	low	low	high	not relevant
IV Worker Safety & Hazard Protection	[23–26]	high	high	low	not necessary
V Task Offloading	[27–31]	medium	medium	high	not relevant
VI Industrial Wearable Systems & Augmented Reality	[32–37]	low	medium	high	essential

*f) Wearable Systems & Augmented Reality:* Industrial wearable systems are the means of human-machine interaction (HMI) for most of the other listed scenario classes. With manufacturing, maintenance, and control still requiring human interaction, wearables present the necessary interface to embedding human workers in smart factories. Wearable systems enable remote control [37], real-time monitoring via augmented reality [36], sensor data aggregation [35], and safety systems [33] while adding the requirements of energy efficiency, size (weight), and wireless networking. Examples roughly follow two streams: human interaction devices and data collection devices [32]. For this scenario class, only the network requirements specific to wearables and augmented reality are considered. If the devices are used for i.e. remote control, Scenario Class II covers the requirements.

### B. Deriving Network Requirements

To derive network requirements for the scenario classes, we need to somewhat generalize the regarded use cases. In the end, it comes down to the specific requirements of the underlying real-time tasks and how messages (i.e. network packets) are integrated into the control flow. The requirements broadly quantified in Table I therefore only give a rough overview of the focal points and limiting factors related to the classes. The spectrum of feasible IIoT scenarios increases with the strictness of real-time guarantees networks can adhere to while not limiting their flexibility. Furthermore, wireless communication technologies that can fulfill these guarantees are the necessary enablers for many of the identified scenarios. Interfacing general IP networking into real-time systems is necessary for use cases requiring external access or cloud computing. However, for most real-time relevant scenarios IT/OT integration is not the enabler. Real-time scenarios become more complex the further away participants are, limiting real-time guarantees and criticality levels.

## III. INDUSTRIAL NETWORKING

The introduction of the first Programmable Logic Controller (PLC), Modicon model 084 in 1969, changed how production systems were designed, implemented, operated, and maintained. Improving mechanical systems and machinery with relay-based control loops was but a small step compared to what PLCs brought to the industry. Whole cabinets of

relays could be replaced with a relatively small number of compact devices saving both space and power. Where the first PLC only had 16 inputs, 16 outputs, and a meager 1 kB of memory, contemporary PLCs have I/O in the order of hundreds, abundant memory, and much higher speeds.

The next sections will cover different industrial networks and common requirements. Table II presents the connection between networks and use cases.

### A. Fieldbuses

With improved industrial automation, communication became an obvious hurdle to tackle. In 1979, Modicon developed and published the serial communication protocol Modbus, an application-layer protocol. Shortly thereafter the work to standardize Profibus started in Germany and was finally published in 1989. These first communication protocols would be the inaugural Operational Technology (OT) networks.

As the first fieldbus protocols grew in popularity, so did issues concerning interoperability. The different protocols were seldom compatible, and few vendors could support multiple protocols. After a somewhat turbulent era often referred to as "the Fieldbus War" [38], an agreement was made in the late 1990s to create a common standard. When the first fieldbus standard (IEC 61158) was published, the final product was essentially a collection of *all* the competing standards at the time. The latest revision of IEC61158 [39] lists 26 different fieldbus protocols grouped into services and protocols. Since then, it has become apparent that the industry is increasingly looking towards open standards [15] to avoid vendor lock-in and a more transparent way to handle security vulnerabilities to name a few.

In this same decade, the Controller Area Network (CAN) was also standardized by the automotive industry. CAN is a serial communication protocol where the message identifier also serves as the message priority. The protocol is optimized for short messages and has the priority encoded in the message identifier. This provides a non-destructive address arbitration which enables messages to pass without any delay induced by lower priority messages.

### B. Packet Switched Networks

At the same time, the IT sector underwent a networking revolution of its own where Ethernet would ultimately end up

as the de-facto standard. After its initial version was published in 1985, it has since moved the throttle from 10 Mbps to 400 Gbps [40] with its sight firmly set on 800 Gbps. Data is split into discrete packets, each identified using a 48-bit Media Access Control (MAC) address giving ample room for growth. To connect hosts, systems can be chained together to form a ring topology or by using ethernet bridges (where store-and-forward switches are the most common). Each frame is individually routed, and the network can quickly adapt to changes in topology and assign new routes to frames while in transit.

In 1974, Cerf et al. published TCP/IP [41] which was to become the backbone of the "network of networks" lovingly called "the Internet". TCP is a connection-oriented protocol that when traffic moves in one direction, control traffic will move both ways allowing TCP to resend lost data and adjust the rate to the slowest link along the path. UDP is the connectionless sibling of TCP without any control traffic and thus offers no indication that traffic arrives at the destination.

1) *Industrial Ethernet*: Industrial Ethernet encompasses the usage of Ethernet in industrial settings. The target applications typically have both latency and reliability requirements, which drives the design of protocols away from traditional Ethernet approaches for collision detection and avoidance. The most common real-time Ethernet protocols are EtherNet/IP<sup>1</sup>, Profinet, and EtherCAT [42]. PROFINET is a translation of PROFIBUS to run over an Ethernet network. EtherCAT is often used in industrial control and automation due to its speed and determinism. TTEthernet is a congestion-free network based on Ethernet that provides Time Triggered service for critical traffic, Rate Constrained for event-triggered traffic as well as a Best-Effort (BE) service. EtherNet/IP is an adaption of DeviceNet to Ethernet, it uses the Common Industrial Protocol (CIP) over TCP and UDP.

2) *Time Sensitive Networking*: (TSN) is a series of IEEE Standards for switched Ethernet [43, 44] where Commercial Off-the-Shelf (COTS) networks can be configured to give bounded latency and extremely low packet loss for critical traffic on the data link layer. TSN removes some of the initial robustness of Ethernet by requiring static routes but gains lower jitter and less out-of-order delivery. In addition, TSN defines strict and fine-grained Quality of Service (QoS) mechanisms which are covered in more detail in Section III-D.

### C. Wireless networks

Wireless sensors are cheaper, easier to install and maintain than their wired counterparts and bear the promise of an infrastructure that is vastly more scalable. In some scenarios, the cost-savings can be as high as 60-90% [45, 46] compared to wired solutions. It can even be the only viable option (e.g., the Tire Pressure Monitoring System (TPMS), tool deflection measurements [47]).

The downside of wireless networks is the shared medium; the integrity of the network is fully dependent upon cooperative participants that only transmit during allocated transmit slots. Frequency bands needed for wireless protocols are a

tightly managed resource, and only a few bands are available for free use, most notably in the 2.4GHz and 5 GHz range. Where a wired network can be fairly resilient to signal interference, have high and predictable bandwidth, and require an adversary to be close to the wired infrastructure to eavesdrop, wireless systems have no such luxury.

Over the years, many wireless protocols have been defined with different characteristics such as high bandwidth, low latency, long-range, a high number of addressable hosts, and robust resistance to interference. Oftentimes, these attributes will be at odds; i.e. with longer ranges come lower bandwidth and higher latency, and high bandwidth can make the traffic more susceptible to interference due to the denser encoding.

Both WirelessHART and ISA 100.11a are common industrial protocols that are based on IEEE 802.15.4 and operate in the unlicensed 2.4GHz frequency band. ZigBee, while also being based on 802.15.4, can be found in some industrial settings but is primarily intended for home automation and low-criticality systems. Bluetooth is mentioned due to its pervasiveness in personal handheld devices. With its low power, it is only capable of transmitting data over a few meters and is primarily intended for short-range personal area networks. The upside is rather low power consumption ample access to complete modules, and comparably high available bandwidth.

In recent years, Wireless LAN (WLAN) has become a common technology in most households, but the technology has not been reliable or deterministic enough for industrial settings. With the recent WLAN6(E), this has improved markedly, and with the availability of Multiple-Input/Multiple-Output (MIMO), access is more reliable and less prone to interference from other senders. The latest version, WLAN6E has also markedly improved the clock accuracy for protocols such as PTP, which makes sensor aggregation more accurate. In addition to the rather crowded 2.4GHz band, WLAN can also operate in the 5GHz and 6GHz range allowing for higher bandwidth at the cost of higher signal attenuation from obstacles along the path.

The fifth generation of mobile telephony (5G) from the 3GPP aims to cover all areas of wireless communications from cellular networks, IoT devices, and industrial networks. 5G is designed to operate in licensed bands where a site license specifying both assigned frequency range and spatial location is required. Interference from other networks should therefore be at a minimum. Three broad use cases have been defined for 5G: cellular data (*enhanced Mobile Broadband, eMBB*), IoT (*massive Machine Type Communications, mMTC*) and low-latency, critical traffic (*Ultra-Reliable, Low Latency, URLLC*). It is important to note that these use cases are not introduced in any single release, but support for each is added as increments with different capabilities in each release. With the first 5G release from 3GPP, Release 15, support for New Radio, rudimentary slicing, and the IoT profile from 4G were among the many parts included. The next release saw the introduction of improved slicing ("VLAN for wireless networks") and redundant transmission for high-reliability communications. Finally, with the latest approved release (Rel17, March 2022), improvements in backhaul networks,

<sup>1</sup>IP is for **Industrial** Protocol.

RAN slicing, public safety, and non-public networks (NPN) have been ratified. NPN is often called “private 5G” and makes it possible to run a 5G network as a standalone network as a local service rather than a public mobile operator. Running a 5G NPN is highly relevant in industrial automation as slicing, URLLC and access to licensed radio bands can greatly aid in security, reliability, and latency. Whereas eMBB is the use case most commonly supported by public providers, URLLC will be most relevant over NPN. Although the specification seems impressive, not much hard data is currently available to evaluate the performance of URLLC.

#### D. Quality of Service

The key strength of Ethernet is its ability to seamlessly accept new systems, adapt to topological changes, and handle variable amounts of traffic. For industrial networks where rigid deadlines are the norm rather than the exception, this dynamism can jeopardize transmission delays and be a major problem. First, packets can take one of multiple *routes* in such a network leading to different arrival orders, variance in delay, or being completely lost. Secondly, once a packet has started transmitting, no other packet, regardless of importance can be transmitted. Since most network bridges are *store and forward*, the entire packet must be fully received before it can be forwarded to the next stop. This requires buffer capacity before newly arrived packets can be forwarded to the next stop. During times of high traffic, these buffers can be exhausted and the bridge will have no other choice than to drop packets.

a) *Standard PSN QoS measures*: QoS describes the treatment of frames belonging to a particular class (or stream) compared to other frames. In this context, a stream, or a flow, is a set of packets that logically belong together and should be treated similarly by the network. Several measures are available, yet whereas these are highly relevant to IT networks and the Internet, fewer apply to the needs of industrial networks.

Differential Services (*DiffServ*) is a highly scalable class-based service where each stream is assigned to a particular service level and it is up to the network administrator to assign resources to each level. DiffServ is intended to be used across large networks and networks of networks where there can be more than one operator. However, the actual service provided to a class may differ between operators. What is more, there is no way to differentiate between streams within a class, meaning as the network grows, the interference from other streams increases.

Integrated Services (*IntServ*) maintains a 1:1 mapping between streams and granted service levels. This ensures consistent QoS throughout the network. Since IntServ is stream-based, its scalability is tied directly to the number of streams. For large networks or networks of networks, the number of active streams will quickly outgrow the available resources in each bridge.

For industrial control applications, the uncertainties of Diff-Serv may not suffice, and for large-scale sensor networks as foreseen in Industry 4.0, IntServ will have scalability problems. An effective solution demonstrated by Harju and Kivimaki [61] is to use IntServ on the edges to shape and

limit all incoming streams, and DiffServ in the core network to handle the bulk of traffic. This hybrid approach can deliver adequate services, especially for large networks, which makes this one of the possible approaches presented by the Deterministic Networking (DetNet) group of IETF.

b) *Time Sensitive Networking*: TSN works by reserving buffer capacity for incoming streams and using different traffic queues on the egress port. An outgoing queue can have a shaper attached to it, which changes the traffic pattern to conform to the desired behavior. The Credit Based Shaper (CBS, [62]) is a *class based* shaper that will group streams for a given traffic class into a single queue. Traffic belonging to this queue is then shaped so that it does not exceed the reserved bandwidth over a short service interval. Since *every* bridge in the domain is required to support these features, the edges will effectively limit the inflow, and the core bridges will work to reduce bursts. CBS is specifically designed to eliminate transient network overloads from bursty traffic and this has been proven to work using Network Calculus [63, 64].

With the Time Aware Shaper (TAS [65]), TSN provides Time Division Multiplexing (TDM) by aligning transmission windows along the path of the traffic. For scheduled traffic (ST) to work, all bridges must be part of a tightly synchronized time domain. When configured properly, TAS can yield extremely low delay variations and give an upper bound of 100  $\mu$ s transmission delay.

However, even with minor time errors, carefully adjusted transmit windows can become desynchronized and effectively delay scheduled traffic for a complete TDM cycle. As the network complexity grows, this problem only worsens. This makes TAS a complex and difficult scheduler to operate and thus suitable for only the most critical streams. It also requires the network to be centrally managed. To allow more sporadic, yet critical traffic and reduce the operational complexity at the same time, a new urgency-based scheduler has been adopted by the working group. The Asynchronous Traffic Shaper [66] has per-class queues and per-stream shaping and uses its internal clock and allows for mixing traffic types such that it can handle sporadic, critical events whilst enforcing rate limits to reduce the impact of bursts. It has been shown that ATS will not increase the worst-case delay [67] of traffic through the network.

CBS is appropriate for traffic that should be regular but occasionally bursty, whereas TAS is best suited for critical traffic that is regular and must be expedited through the network. For important, yet sporadic or aperiodic traffic (e.g. monitor alarms, events), ATS is appropriate.

It is worth noting that the reservation of streams may fail if one or more bridges are unable to accommodate the requirements and that can only reliably be detected at runtime. It is possible to discover this *a priori* to a certain extent (Maile et al. [64]), but as small changes to the network can result in new routes for traffic, previous scenarios may no longer be possible. This makes it difficult to realize the full potential of a network using a fully distributed model where each node announces or reserves resources for a stream individually. Instead, a centralized controller can handle end-station interaction and bridge configurations. The *Centralized*

TABLE II  
TECHNOLOGIES ALONG SECURITY, DETERMINISM, AND BANDWIDTH. LEGEND: ✓: WELL SUITED, ✗: NOT WELL SUITED

	Security	Determinism	Bandwidth	Relevant Scenarios					
				I	II	III	IV	V	VI
<i>Fieldbuses</i>									
CAN	E	10 ms	1 Mbps	[48, 49]	✗	✓	✗	✓	✗
CAN-FD	E	100 $\mu$ s	5 Mbps	[50]	✗	✓	✗	✓	✗
Modbus	E	10 ms	115 kbps	[49]	✗	✓	✗	✓	✗
PROFIBUS	E	10 ms	12 Mbps	[49, 51]	✗	✓	(✓)	✓	(✓)
<i>Wired network</i>									
Modbus TCP	E	45 $\mu$ s (ideal conditions)	100 Mbps	[52]	✗	(✓)	✓	✓	✗
PROFINET	E	10-100 ms	1 Gbps	[53]	✗	(✓)	✓	(✓)	✓
EtherNet/IP	E	1-2 ms	1 Gbps	[54]	✗	✓	✓	✓	✗
TSN CBS	E,A	2 / 50 ms	40 Gbps	[55]	✗	(✓)	✓	✓	✗
EtherCAT	E	34 $\mu$ s	10 Gbps	[56]	✗	✓	✗	✓	(✓)
TTEthernet	E,A	low, $\mu$ s (offline schedule)	1 Gbps	[55]	✗	✓	✓	✓	✗
TSN ST	E,A	100 $\mu$ s	40 Gbps	[55]	✗	✓	(✓)	✓	(✓)
<i>Wireless network</i>									
WirelessHART	I,C,A	10 ms	250 kbps	[57]	✓	(✓)	✗	(✓)	✓
ISA 100.11a	I,C,A	10 ms	250 kbps	[57]	✓	(✓)	✗	(✓)	✓
Bluetooth 5.0	I,C,A	10-100 ms	48 Mbps	[58]	✗	✗	✓	✗	(✓)
WLAN 6	I,C,A	1 ms (ideal conditions)	9.6 Gbps	[59, 60]	(✓)	✗	✓	✗	(✓)
5G eMBB	I,C,A	10-100 ms	10 Gbps	[60]	✗	✗	✓	✗	(✓)

*User Configuration* (CUC) and *Centralized Network Configuration* (CNC) provide single points of contact for end-stations. New streams are evaluated and by using the total overview, an optimal path can be created and forwarded to the CNC, which in turn configures all the required bridges before the end stations are notified and traffic can begin. For TAS, such a centralized controller is a requirement.

#### E. Common Network Requirements for Industrial Automation

Devan et. al [68] list 4 criteria as fundamental for a wireless industrial network: 1) Secure against malicious intruders and misconfigured devices, 2) easy and dependable access to sensor data, 3) Interoperability between vendors and protocols, and 4) active research community to adapt and grow to future needs. Missing in this list is the need for deterministic transport. From the discussion in Section III-D, we can extend this list to also include wired industrial networks and include bounded latency and time synchronization as relevant metrics.

An updated requirement is thus:

- **Open Standards** Available standards and royalty-free technology should be the preferred approach as this will allow for better interoperability between vendors and a more open community that encourages academic research.
- **Security** Not only should the content be shielded from external eyes, but the network should be able to detect if traffic has been altered, delayed, or injected into the network by a third party.
- **Reliability and Availability** Network delivery must be reliable in that once sent, the sender should be confident that it will arrive at the destination within a known time frame. At the same time, a sender should expect the network to be available to accept new data within the pre-defined constraints (not overstepping BW bounds, etc.). The network should also be robust against jamming and other malicious attempts to disrupt the service [69]

- **Latency** Especially closed control loops are sensitive to delay variations, but for any streams, expecting delivery within a certain time frame is a requirement.
- **Time synchronization** As networks are used to build distributed systems, a shared understanding of time (what is often called a shared time domain) is needed. The accuracy of the domain is dependent upon how well the network can forward time synchronization messages.

In Table II, the most common solutions found in industrial networks are listed. Each is briefly evaluated along 3 common axes: 1) Security, 2) Determinism (i.e. jitter), and 3) Bandwidth (upper limit). For brevity, Reliability, Availability, and Latency have been combined into “Determinism” as all the aforementioned requirements will directly affect the determinism of the traffic. Security can be further divided into *i*) **External**: the protocol relies on external security measures, *ii*) **Integrity**: messages are accompanied by robust checksums to detect modification, *iii*) **Confidentiality**: each message is encrypted using a secret known only to authorized parties, *iv*) **Secure Authentication and Authorization**: each node on the system must be securely identified before being granted access to the network <sup>2</sup> In addition, each row is weighted against the list of use cases in Table I with ✓ indicating a good fit, ✗ a poor. A (✓) indicates that the protocol can support it under ideal conditions, but it is not well suited. Likewise, (✗) indicates that the protocol *can* be made to work, but it is probably not a great idea.

#### IV. ONGOING EFFORTS TOWARDS REAL-TIME NETWORKS

When it comes to the inherent predictability requirements of real-time applications, packet-switched networking alone is not adequate. This is because the load on individual network hardware in larger networks is unpredictable, and packet

<sup>2</sup>Both wired and wireless Ethernet can achieve better security by including standards such as Port-based authentication (802.1X) and Secure Device Identity (802.1AR).

transmission times (as well as routes) are variable. In addition, the packet loss rates of wireless transmissions are always difficult to account for. As described in the previous section, there are industry standards that address these issues, either by sticking to packet-less bus communication or by adding specific real-time capabilities to Ethernet. However, with the convergence of IT and OT networks, as well as the highly mobile nature of the IIoT scenarios mentioned above, further real-time networking solutions need to be found.

In this section, we present recent work on real-time IIoT networking. We consider peer-reviewed articles and papers from the last 5 years. The works can be either novel techniques, adaptations, or evaluations of existing standards optimized for real-time IIoT scenarios. The reviewed works are divided into subsections of equal levels of abstraction and underlying technologies. Table III compares the works qualitatively concerning their scope and applicability to our scenario classes. Entries marked with  $\checkmark$  or  $\times$  determine whether the work is feasible for the scenario class. Entries marked with  $\bullet$  are works that do not directly facilitate a scenario class but also do not prohibit it. It also indicates the type of source institution (academic or industry) and whether the work supports wireless communication.

#### A. Network Architectures

The field of research with the broadest scope regards network architectures for real-time IIoT environments. Next to architectures realized by SDN, this segment also includes research on IT/OT integration and OPC UA.

In [70] Ishtaque ul Huque et al. present a system architecture for time-sensitive heterogeneous wireless distributed software-defined networks. They derive this system architecture from enabling state-of-the-art technologies and their requirements. Besides the manageability of parameters in heterogeneous networks, the authors hope to facilitate TSN integration with legacy networks.

Kiangala and Wang combine zero-loss redundancy protocols, TSN, and edge computing concepts to realize an intra-domain network architecture attending to the reliability and predictability needs of time-critical IIoT applications [71]. Their solution is entirely based on IP networking. Instead of manageability via SDN they focus on technological implementations for high reliability and determinism.

Network architectures have been a focus in recent works primarily due to the IT/OT convergence requirements of Industry 4.0 and IIoT applications. Foschini et al. present an SDN-enabled architecture for this and analyze its behavior during DDoS attacks [72]. With a multi-layered network architecture, they aim to provide layer-specific security and real-time properties while making data from IIoT devices usable inside the business network of an industrial plant with autonomous vehicles. Within their DDoS attack, they showed that mere changes to the network architecture cannot secure the highly critical lower levels of the network (i.e. physical machines).

The Open Platform Communication Unified Architecture (OPC UA) was introduced in 2008 as an interoperability

standard for reliable information exchange and has gained momentum with discussions on IIoT networks. In recent years Li et al. presented an OPC UA architecture with TSN capabilities for the IIoT [73] and Morato et al. published a general assessment of OPC UA implementations under current Industry 4.0 requirements [74]. Both works showed that OPC UA can be used to integrate real-time communication requirements into Ethernet-based networks in the manufacturing industry.

#### B. SDN

When industrial networks become more complex and contain mixed computing systems and real-time requirements Software-Defined Networking can help with managing the resulting heterogeneity. Wang and Li present an SDN-based solution for task offloading in IIoT environments [75]. A computing mode selector is implemented in the SDN controller and offloaded tasks are given priority based on real-time parameters. The network transmits offloaded tasks to fog computing resources in order of this priority.

Another solution that addresses mixed timing criticality in large networks is proposed by Lin et al. [76]. SDN is used to implement a traffic engineering approach to schedule the transfer of delay-sensitive traffic. This works using real-time analysis of the network and monitoring the QoS metrics of participating links. Based on these metrics a dynamic scheduler with multi-path routing capabilities manages the flows.

Zeng et al. address flaws of Industrial Ethernet, namely poor scalability, insufficient self-configuration capabilities, and increased costs due to the use of proprietary hardware and present a time-slotted software defined Industrial Ethernet [77]. The approach contains a time synchronization mechanism based on PTP and a system architecture for time slot-based industrial switches. Using SDN, the implementation becomes scalable, and reconfigurable, and is not dependent on frequent infrastructure changes.

#### C. TSN

In recent years, researchers have addressed various shortcomings of TSN by extending, improving, and integrating it with other systems and frameworks. Schriegel and Jasperneite worked on a bridging mode called Time-Aware Forwarding (TAF) [78] to increase the flexibility of TSN and thereby accelerate the migration from Profinet to TSN in industrial communication. With the approach, already existing networking hardware can be made compatible with TSN.

Tackling the scheduling of time-triggered traffic in TSN, Bujosa et al. present Hermes, a heuristic multi-queue scheduler [79]. With this improvement to the synthesis algorithm of gate control lists in TSN networks, they increase network scalability by reducing its scheduling complexity.

To control network jitter, incoming packets are buffered along the routing path in a TSN network. Chaine et al. propose a solution *Egress TT* that performs this buffering only at the final network node [80] and optimizes it for network scalability. The solution allows to use of non-TSN networking

TABLE III  
RECENT WORKS

Work	Scope	Issue(s) addressed	Source	I	II	III	IV	V	VI	Wireless
[70]	SDN architecture	IT/OT; flexibility	academia	●	X	✓	X	✓	●	✓
[71]	IP architecture	reliability & determinism	academia	X	✓	●	✓	✓	X	X
[72]	SDN architecture	IT/OT; security	academia	X	X	✓	X	✓	X	X
[73]	OPC UA	TSN integration	academia	X	✓	✓	●	●	X	X
[74]	OPC UA	TSN assessment	academia	X	✓	✓	●	●	X	✓
[75]	SDN for IIoT	offloading	academia	X	●	✓	X	✓	X	✓
[76]	SDN for traffic engineering	delay sensitivity	academia	X	✓	X	✓	●	X	X
[77]	SDN industrial Ethernet	flexibility; determinism; scale	academia	X	✓	✓	●	✓	X	X
[78]	Time-aware forwarding	Profinet/TSN migration	academia	X	✓	✓	✓	●	X	X
[79]	TSN scheduler	scalability	academia	X	●	✓	●	✓	X	X
[80]	TSN traffic shaping	scalability; complexity	aviation	X	●	✓	X	✓	X	X
[81]	OPC UA with TSN	network infrastructure	automation	X	✓	✓	✓	✓	X	X
[82]	TSN using DDS	heterogeneous TSN; flexibility	academia	X	●	✓	✓	X	X	✓
[83]	Wireless TSN	determinism; reliability	chip manufacturer	✓	✓	✓	●	X	✓	✓
[84]	Link layer/application mapping	wireless TSN applicability	chip manufacturer	✓	✓	✓	●	X	✓	✓
[85]	RT-WiFi over SDR	determinism; flexibility	academia	✓	✓	✓	●	X	✓	✓
[86]	5G slicing management	determinism; isolation	telecom	●	●	●	✓	✓	✓	✓
[87]	5G private networks	assessment	telecom	●	●	●	●	●	●	✓
[88]	5G private networks	assessment	telecom/car	●	●	●	●	●	●	✓
[89]	RT-aware packet reception	determinism	academia	X	✓	✓	●	●	X	✓
[90]	RT-aware NIC	determinism	academia	X	✓	✓	●	●	X	✓
[91]	RT-aware MAC filtering	determinism	academia	X	✓	✓	●	●	X	✓
[92]	Timed C extension	TSN-aware applications	academia	X	✓	✓	✓	●	X	X

on the routing path and reduces computational complexity while somewhat increasing latencies.

In [81], Bruckner et al. showed how the ubiquitous OPC-UA protocol benefits from using TSN. Similarly, in [82] Agarwal et al. demonstrated improved reliability and reduced delay for Data Distribution Services (DDS) when TSN was used to protect and expedite the traffic through the network.

#### D. Real-Time Aware Wireless Technologies

The need for reliable and deterministic wireless communication can be derived from most scenarios presented in Section II. The following works from the past years attend to real-time wireless communication.

A seemingly natural step is to transfer TSN methods to work with wireless technologies. The concomitant challenges and research objectives have been thoroughly investigated by Cavalcanti et al. [83]. Next to a comprehensive overview of state-of-the-art wireless technologies and IEEE 802.1 TSN standards, they discuss new approaches on top of next-generation wireless technologies (e.g. WiFi 6, WigGig, and 5G) to overcome the radio-inherent challenges concerning packet loss and jitter.

Sudhakran et al. build on top of this work and present a methodology to map application layer timing requirements in a collaborative robot application to the link layer, based on wireless TSN over WiFi [84]. Rather than going further into the TSN standards, they address how to classify traffic, extract time-critical flow parameters, and define an efficient schedule for the end-to-end QoS approach.

Yun et al. recognize the older real-time aware WiFi (RT-WiFi [93]) technology which is implemented on common off-the-shelf hardware and hence hard to update and maintain. In their work, they propose a software-defined radio approach of RT-WiFi implemented on an FPGA called SRT-WiFi [85].

They provide a fully open system architecture and perform extensive evaluations on a multi-cluster SRT-WiFi testbed.

#### E. Fifth Generation Mobile Networks

The fifth generation of mobile networking (5G) promises several improvements and enabling technologies for Industry 4.0 and smart factory applications. Among them are network slicing, private management, and ultra-low latencies.

Network slicing allows for logically separated virtual networks over the same physical 5G network. Both, the integration of different business layers as well as connection-specific latency control could be realized with this. Walia et al. studied the usage of network slicing in a smart factory and developed a management model for 5G slicing in the domain [86]. As the effective usage of 5G for Industry 4.0 environments requires self-managed or "private" 5G networks, some recent works have focused on their implementation and feasibility. Ajiaz et al. present an overview of the motivation behind and functions of private 5G networks [87]. They present a large number of potential use cases and benefits for the IIoT and portray private 5G networking as the future of industrial networks. Wen et al. come to a similar conclusion while pointing out the early stage at which private 5G networking currently is [88]. Actual implementation and management are currently only feasible for large companies with a networking background. In their paper covering critical mMTC, Pokhrel et al. [94], argue that although URLLC is capable of providing excellent real-time behavior, the cost of doing so means relatively few devices can be connected in such a fashion. Similarly, where mMTC is capable of connecting a plethora of devices, the individual QoS is not compatible with sensor networks. To be able to meet the need for a large, wireless sensor network, they propose "critical mMTC".

### F. Device-Layer Technologies

Only a few works have considered making improvements to the lowest layer in IIoT networks. The following research papers are concerned with securing embedded devices that are (somewhat newly) connected to large networks and responsible to execute real-time tasks. Blumschein et al. present a real-time aware IP networking stack for IoT devices [95]. By classifying packets as early as possible and inheriting real-time task priorities to the networking task, they prevent priority inversions between a high-priority task and the processing of lower-priority packets. Additionally, incoming packet rates are limited to prevent a system overload from incoming packets.

In [90] a hardware-based approach with similar goals is presented. Using a multi-queue NIC design, packets are reordered and filtered based on the priority of the receiving real-time task. Furthermore, real-time aware interrupt moderation is proposed that reduces the number of interrupts generated by incoming traffic while guaranteeing low latencies for high-priority packets. A SW/HW co-design for real-time aware packet reception is presented in [89].

Johansson et al. use MAC layer filtering to mitigate the effects of best-effort traffic reception on real-time tasks [91]. They extend the network driver of VxWorks to support multiple receive queues and an interface that supports the configuration of the Ethernet Controller's MAC filter. This way, packets are filtered and enqueued based on their priority in hardware, making it possible to treat incoming traffic based on real-time considerations.

In [92], TSN was used to extend Timed C, an extension to the C programming language, and include network channels as a primitive in the language. When faced with large network loads, the critical traffic was reliably forwarded with minimal delay and jitter demonstrating the usefulness of TSN in distributed real-time systems.

## V. DISCUSSION

Traditionally, industrial networks have been isolated, mostly homogeneous, and designed with dedicated protocols and hardware to meet stringent reliability and real-time requirements. With the coming transformation of Industry 4.0 and IT/OT convergence, industrial networks need to become more configurable and flexible, enabling a wider range of applications than before. This, of course, requires tighter connectivity between networked systems, as well as a higher degree of dynamism for nodes joining and leaving the network.

### A. Bridging the Gap between IIoT Scenarios and Network Requirements

Looking at Table II, the wireless networking requirements of Scenario Classes I and VI appear to be the most difficult to meet. While several wireless communication standards exist, they either cannot meet the strict latency predictability requirements or cannot meet the bandwidth requirements of multimedia data. Once high reliability and latency are taken into account, current wireless networks do not scale sufficiently, i.e., a research gap exists where critical real-time requirements meet a need for wireless communication. Current

wireless real-time protocols are generally unable to scale to the required size and the aggregated bandwidth expected in the coming years. Similarly, WLAN, and especially WLAN6E, can be seen as an attractive alternative with high bandwidth, low latency, improved timing accuracy, and readily available COTS hardware.

Comparing this to Table III, it can be seen that this is where wireless TSN technologies will play a significant role in enablement. The main gap-filler distilled from this work is wireless technologies that can provide a measure of predictability. However, the overall feasibility of this must be viewed with caution. While latency guarantees can be improved by real-time aware wireless packet switching, the inherent unpredictability of radio must not be overlooked.

While privately managed 5G networks seem to be a part of the solution, the high complexity and cost make it impractical for many companies and use cases.

The presented works regarding wired networks show that “real-time networks” are more static and carefully planned than traditional IT networks tend to be. Even though technologies such as TSN help bring determinism to COTS Ethernet, achieving high flexibility and reconfigurability is a largely unsolved challenge. Combining TSN with its centralized controllers (CNC, CUC) and SDN is one promising avenue that would extend to both WLAN and 5G solutions. The downside of such a solution is the vast complexity of all systems; needless to say, the factory network of the future will be almost unrecognizable from today’s, and be a major asset of its own.

Standardization and holistic large-scale implementations also are open challenges to the remaining subfields. Even where research papers are feasible for specific scenario class requirements these only focus on individual aspects. The feasibility of the presented approaches still has to be validated in complex engineered systems. Industry 4.0 is still missing a fixed set of standards and technologies which will be important for trust in safety and reliability. The approaches from the works presented have to be merged and implemented in holistic system architectures including all actors of the network, from embedded real-time devices, network devices, and compute nodes such as edge servers and cloud systems.

## VI. RELATED WORK

Several other works have looked at network requirements for industrial use cases. In the following, we present a selection of surveys from the past years that compare and analyze industrial networking solutions.

Xu et al. [96] surveyed IIoT research from a systems perspective in 2018. In their work, they divide the wide research area into the three key aspects of control, networking, and computing before categorizing and investigating related works. While incorporating networking they do not cater to any real-time requirements. A more real-time focused survey was presented by Kim et al. [97] in 2017. In their work, the authors analyzed real-time communication in wireless sensor networks, which are in large part relevant to IIoT scenarios. Another survey on IIoT research was presented by Sisinni et al. [98] in 2018 with a focus on open challenges. Next to the

need for energy efficiency, coexistence, interoperability, and security they also identify real-time performance as a future research challenge.

Park et al. [99] presented requirements and challenges with using wireless networks in control applications. In particular, the focus lies on network design and relevant protocols. Key benefits such as ease of installation and reduced operating costs are discussed. Several use cases, both relevant to current technologies (e.g. building automation, tire pressure sensors, wireless sensor coverage in industrial applications) and more futuristic examples where the avionics are brought out as an example where reducing cabling can provide 2-5% weight reduction alone. As wireless networks cannot provide the same isolation from interference as corresponding wired technologies, control loops must be adapted to tolerate packet loss and variable delays. A joint design approach where control loops and the wireless network are jointly optimized to arrive at an acceptable performance is presented as one promising approach to improve the performance of wireless control systems.

In [100], Zunino et al. investigate the status of network technologies relevant to the Industrial Internet, or Industry 4.0. They find that although most technologies needed to realize Industry 4.0 are present, they fall short on flexibility, scalability, reliability, real-time behavior, and security, to name a few. A key point is to realize that "Industry 4.0" is a reaction to the change in market demands especially seen in developed countries. A shorter time to market, a higher degree of customization, and small production batches are brought forward as key enablers to stay competitive. To realize this, production lines must be highly configurable, have a high degree of situational awareness, and be extremely energy efficient. Where current OT systems are tailored specifically for a particular task and hard real-time requirements are met by careful analysis and provisioning, future networks cannot be designed with such static scenarios in mind. The communications networks must be able to provide real-time guarantees to a subset of nodes whilst also providing other QoS levels for various nodes, sensors, and systems.

Chen et al. [101] argue how smart manufacturing must use wireless technologies to orchestrate multi-robot systems to obtain the needed flexibility. The third industrial revolution improved the flexibility of the *quantity* produced, with the fourth, the flexibility of type, quantity, and quality being at the center of attention. To change the production setup in such fundamental ways means that multi-robot systems must be highly configurable, the network must adapt to varying loads, and automated delivery systems like AGVs must be just as adaptable.

## VII. SUMMARY

Real-time demands on networks in industrial environments have risen with the advent of the IoT paradigm and Industry 4.0. In this paper, we have listed common and anticipated use cases for industrial networks and identified the criteria needed to meet the requirements of each. We reviewed established industrial networking technologies and protocols and presented

current academic works regarding the topic. By comparing different networking technologies to these criteria and use cases, we hope to give an overview of challenges and solutions concerning IIoT scenarios from a real-time networking perspective.

## REFERENCES

- [1] Elena Simona Lohan et al. "Benefits of positioning-aided communication technology in high-frequency industrial IoT". In: *IEEE Communications Magazine* 56.12 (2018).
- [2] Wanchun Liu et al. "On the latency, rate, and reliability tradeoff in wireless networked control systems for IIoT". In: *IEEE Internet of Things Journal* 8.2 (2020).
- [3] Xuegang Zhan et al. "Industrial internet of things and unsupervised deep learning enabled real-time occupational safety monitoring in cold storage warehouse". In: *Safety Science* 152 (2022).
- [4] Helge Nordal and Idriss El-Thalji. "Modeling a predictive maintenance management architecture to meet industry 4.0 requirements: A case study". In: *Systems Engineering* 24.1 (2021).
- [5] Richard Blake, Lucia Michalkova, and Yuriy Bilan. "Robotic wireless sensor networks, industrial artificial intelligence, and deep learning-assisted smart process planning in sustainable cyber-physical manufacturing systems". In: *Journal of Self-Governance and Management Economics* 9.4 (2021).
- [6] Akseer Ali Mirani et al. "Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review". In: *Sensors* 22.15 (2022).
- [7] Jan Hicking, Max-Ferdinand Stroh, and Sebastian Kremer. "Collaboration Through Digital Integration—An Overview of IT-OT-Integration Use-Cases and Requirements". In: *Working Conference on Virtual Enterprises*. Springer, 2021.
- [8] Lianbo Ma et al. "TCDA: Truthful combinatorial double auctions for mobile edge computing in industrial Internet of Things". In: *IEEE Transactions on Mobile Computing* (2021).
- [9] Zoran Miljković et al. "New hybrid vision-based control approach for automated guided vehicles". In: *The International Journal of Advanced Manufacturing Technology* 66.1 (Apr. 2013).
- [10] Ajay K. S. Singholi, Mamta Mittal, and Ankur Bhargava. "A Review on IoT-Based Hybrid Navigation System for Mid-sized Autonomous Vehicles". In: *Advances in Electromechanical Technologies*. Ed. by V. C. Pandey, P. M. Pandey, and S. K. Garg. Lecture Notes in Mechanical Engineering. Springer, 2021.
- [11] Suresh Chavhan, Ravi Arun Kulkarni, and Atul Ramesh Zilpe. "Smart Sensors for IIoT in Autonomous Vehicles: Review". In: *Smart Sensors for Industrial Internet of Things: Challenges, Solutions and Applications*. Ed. by Deepak Gupta et al. Internet of Things. Springer, 2021.

- [12] Lucia Lo Bello and Wilfried Steiner. "A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems". In: *Proceedings of the IEEE* 107.6 (June 2019).
- [13] Mohammadreza Barzegaran et al. "Fogification of electric drives: An industrial use case". In: *25th International Conference on Emerging Technologies and Factory Automation (ETFA)*. Vol. 1. IEEE, 2020.
- [14] Roman Zhohov et al. "Real-time Performance Evaluation of LTE for IIoT". In: *43rd Conference on Local Computer Networks (LCN)*. IEEE, Oct. 2018.
- [15] Hakan Kayan et al. "Cybersecurity of industrial cyber-physical systems: a review". In: *ACM Computing Surveys (CSUR)* 54.11s (2022).
- [16] Martin Kajan et al. "Control of automated guided vehicle with PLC SIMATIC ET200S CPU". In: *American Journal of Mechanical Engineering* 1.7 (2013).
- [17] Kang Huang et al. "To Sense or to Control: Wireless Networked Control Using a Half-Duplex Controller for IIoT". In: *Global Communications Conference (GLOBECOM)*. IEEE, 2019.
- [18] R Bock, KR Uren, and G van Schoor. "Performance impact of network conditions on an IIoT system." In: *Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA)*. IEEE, 2021.
- [19] Ameeth Kanawady and Aditya Sane. "Machine learning for predictive maintenance of industrial machines using IoT sensor data". In: *8th International Conference on Software Engineering and Service Science (ICSESS)*. IEEE, Nov. 2017.
- [20] Javier Silvestre Blanes et al. "802.11n Performance analysis for a real multimedia industrial application". In: *Computers in Industry* 66 (Jan. 2015).
- [21] Zafar Iqbal, Kiseon Kim, and Heung-No Lee. "A Cooperative Wireless Sensor Network for Indoor Industrial Monitoring". In: *IEEE Transactions on Industrial Informatics* 13.2 (Apr. 2017).
- [22] Marouane Salhaoui et al. "Smart industrial iot monitoring and control system based on UAV and cloud computing applied to a concrete plant". In: *Sensors* 19.15 (2019).
- [23] Tommi Kivelä, Markus Golder, and Kai Furmans. "Towards an approach for assuring machinery safety in the IIoT-age". In: *Logistics Journal: Proceedings* 2018.01 () .
- [24] C Zhou et al. "Industrial Internet of Things:(IIoT) applications in underground coal mines". In: *Mining engineering* 69.12 (2017).
- [25] M McNinch et al. "Leveraging IIoT to improve machine safety in the mining industry". In: *Mining, metallurgy & exploration* 36.4 (2019).
- [26] Miguel Angel Reyes, Grant W King, and Gregory G Miller. "Intelligent machine guard monitoring: A wireless system to improve miner safety". In: *IEEE Industry Applications Magazine* 20.2 (2013).
- [27] Zicong Hong et al. "Multi-Hop Cooperative Computation Offloading for Industrial IoT–Edge–Cloud Computing Environments". In: *IEEE Transactions on Parallel and Distributed Systems* 30.12 (Dec. 2019).
- [28] Ilja Behnke et al. "Offloading Real-Time Tasks in IIoT Environments under Consideration of Networking Uncertainties". In: *2nd International Workshop on Middleware for the Edge (MiddleWEdge) at Middleware '23*. ACM, 2023.
- [29] Xiaoheng Deng et al. "Intelligent Delay-Aware Partial Computing Task Offloading for Multi-User Industrial Internet of Things through Edge Computing". In: *IEEE Internet of Things Journal* (2021).
- [30] Jincheng Xu et al. "Joint Task Offloading and Resource Allocation for Multi-Hop Industrial Internet of Things". In: *IEEE Internet of Things Journal* (2022).
- [31] Junchao Ma et al. "Reliability Versus Latency in IIoT Visual Applications: A Scalable Task Offloading Framework". In: *IEEE Internet of Things Journal* (2022).
- [32] Xiang T. R. Kong et al. "Industrial wearable system: the human-centric empowering technology in Industry 4.0". In: *Journal of Intelligent Manufacturing* 30.8 (Dec. 2019).
- [33] Ekaterina Svertoka et al. "Wearables for Industrial Work Safety: A Survey". In: *Sensors* 21.11 (Jan. 2021).
- [34] Mario Lorenz, Sebastian Knopp, and Philipp Klimant. "Industrial Augmented Reality: Requirements for an Augmented Reality Maintenance Worker Support System". In: *International Symposium on Mixed and Augmented Reality Adjunct*. IEEE, 2018.
- [35] Jonathan Rosales, Sourabh Deshpande, and Sam Anand. "IIoT based Augmented Reality for Factory Data Collection and Visualization". In: *Procedia Manufacturing*. 49th SME North American Manufacturing Research Conference (NAMRC 49, ) 53 (Jan. 2021).
- [36] Jordi Mongay Batalla. "On Analyzing Video Transmission Over Wireless WiFi and 5G C-Band in Harsh IIoT Environments". In: *IEEE Access* 8 (2020).
- [37] Yijun Li et al. "Helically Intersected Conductive Network Design for Wearable Electronic Devices: From Theory to Application". In: *ACS Applied Materials & Interfaces* 13.9 (2021).
- [38] Max Felser. "The fieldbus standards: History and structures". In: *Technology Leadership Day* (Jan. 2002).
- [39] IEC. *Industrial communication networks - Fieldbus specifications*. International Standard. Geneva, CH: International Electrotechnical Commission, Apr. 2019.
- [40] David J. Law et al. "IEEE Standard for Ethernet". In: *IEEE Std 802.3-2022* (2022).
- [41] V Cerf, Y Dalal, and C Sunshine. *Specification of Internet Transmission Control Program*. RFC 675. Dec. 1974.
- [42] Thomas Watteyne et al. "Industrial Wireless IP-Based Cyber –Physical Systems". In: *Proceedings of the IEEE* 104.5 (May 2016).

- [43] Tony Jeffree, Paul Congdon, and Michael Johass Teener. “IEEE Standard for Local and Metropolitan Area Networks—Audio Video Bridging (AVB) Systems”. In: *IEEE Std 802.1BA-2021* (2021).
- [44] “IEEE Standard for Local and Metropolitan Area Network—Bridges and Bridged Networks”. In: *IEEE Std 802.1Q-2018* (2018), pp. 1–1993.
- [45] Robb Sparks. “Reduce Costs with Wireless Instrumentation”. In: *POWER Magazine* (2009).
- [46] Guodong Zhao et al. “Toward Real-Time Control in Future Wireless Networks: Communication-Control Co-Design”. In: *IEEE Communications Magazine* 57.2 (2019).
- [47] Dan Östling et al. “Cutting process monitoring with an instrumented boring bar measuring cutting force and vibration”. In: *Procedia CIRP*. 8th CIRP Conference on High Performance Cutting 77 (Jan. 2018).
- [48] Eduardo P. Godoy et al. “Design of CAN-based Distributed Control Systems with Optimized Configuration”. In: *Journal of the Brazilian Society of Mechanical Sciences and Engineering* 32 (Dec. 2010).
- [49] M.D. Rubio Benito et al. “Performance Evaluation of Four Field Buses”. In: *1999 7th IEEE International Conference on Emerging Technologies and Factory Automation. Proceedings ETFA '99 (Cat. No.99TH8467)*. Vol. 2. 1999.
- [50] Carina Austermann and Stephan Frei. “Concepts for Bitrate Enhancement and Latency Reduction in Recurring Disturbed CAN FD Networks”. In: *International Symposium on Electromagnetic Compatibility - EMC EUROPE*. Sept. 2020.
- [51] Tao Jun and Wang Zhan-lin. “Analysis of PROFIBUS-DP Network Delay and Its Influence on the Performance of Control Systems”. In: *Wuhan University Journal of Natural Sciences* 10.5 (Sept. 2005).
- [52] Susanne Kenner et al. “Comparison of smart grid architectures for monitoring and analyzing power grid data via Modbus and REST”. In: *EURASIP Journal on Embedded Systems* 2017 (Aug. 2016), p. 12.
- [53] *PROFINET Communication Channels*. <https://profinetuniversity.com/profinet-basics/profinet-communication-channels/>. Accessed: 2023-09-30.
- [54] E. Alessandria, L. Seno, and S. Vitturi. “PERFORMANCE ANALYSIS OF ETHERNET/IP NETWORKS”. In: *IFAC Proceedings Volumes*. 7th IFAC Conference on Fieldbuses and Networks in Industrial and Embedded Systems 40.22 (Jan. 2007).
- [55] Luxi Zhao et al. “Timing analysis of rate-constrained traffic in TTEthernet using network calculus”. In: *Real-Time Systems* 53 (2017).
- [56] Vinh Quang Nguyen and Jae Wook Jeon. “EtherCAT Network Latency Analysis”. In: *International Conference on Computing, Communication and Automation (ICCCA)*. Apr. 2016.
- [57] Eduardo Paciência. Godoy, Fernando Scorzoni, and Arthur José Vieira Porto. “Evaluating Serial ZigBee Devices for Application in Wireless Networked Control Systems”. In: *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society*. Oct. 2012.
- [58] Raúl Rondón, Mikael Gidlund, and Krister Landernäs. “Evaluating Bluetooth Low Energy Suitability for Time-Critical Industrial IoT Applications”. In: *International Journal of Wireless Information Networks* 24.3 (Sept. 2017).
- [59] Dmitry Bankov et al. “Enabling Real-Time Applications in Wi-Fi Networks”. In: *International Journal of Distributed Sensor Networks* 15.5 (2019).
- [60] Edward J. Oughton et al. “Revisiting Wireless Internet Connectivity: 5G vs Wi-Fi 6”. en. In: *Telecommunications Policy* 45.5 (2021).
- [61] J. Harju and P. Kivimaki. “Co-operation and comparison of DiffServ and IntServ: performance measurements”. In: *Proceedings 25th Conference on Local Computer Networks. LCN*. IEEE, Nov. 2000.
- [62] Tony Jeffree et al. “IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks Amendment 14: Stream Reservation Protocol (SRP)”. In: *IEEE Std 802.1Qat-2010* (2010).
- [63] Joan Adrià Ruiz De Azua and Marc Boyer. “Complete modelling of AVB in network calculus framework”. In: *Proceedings of the 22nd International Conference on Real-Time Networks and Systems*. 2014.
- [64] Lisa Maile, Kai-Steffen Hielscher, and Reinhard German. “Network calculus results for TSN: An introduction”. In: *Information Communication Technologies Conference (ICTC)*. IEEE. 2020.
- [65] Michael Johas Teener, János Farkas, and TSN WG. “IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic”. In: *IEEE Std 802.1Qbv-2015* (2016). Ed. by Tony Jeffrey.
- [66] Johannes Specht and Soheil Samii. “Urgency-based scheduler for time-sensitive switched ethernet networks”. In: *2016 28th Euromicro Conference on Real-Time Systems (ECRTS)*. IEEE. 2016.
- [67] Ahmed Nasrallah et al. “Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research”. In: *IEEE Communications Surveys & Tutorials* 21.1 (2019).
- [68] P. Arun Mozhi Devan et al. “A Survey on the Application of WirelessHART for Industrial Process Monitoring and Control”. In: *Sensors* 21.15 (Jan. 2021).
- [69] Hossein Pirayesh and Huacheng Zeng. “Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey”. In: *IEEE Communications Surveys & Tutorials* 24.2 (2022).
- [70] Tanvir Ishtaique ul Huque et al. “A system architecture for time-sensitive heterogeneous wireless distributed software-defined networks”. In: *2019 Military Communications and Information Systems Conference (MilCIS)*. Nov. 2019.
- [71] Kahiomba Sonia Kiangala and Zenghui Wang. “An Effective Communication Prototype for Time-Critical IIoT Manufacturing Factories Using Zero-Loss Redundancy Protocols, Time-Sensitive Networking, and

- Edge-Computing in an Industry 4.0 Environment". In: *Processes* 9.11 (Nov. 2021).
- [72] Luca Foschini et al. "An SDN-Enabled Architecture for IT/OT Converged Networks: A Proposal and Qualitative Analysis under DDoS Attacks". In: *Future Internet* 13.10 (2021).
- [73] Yuting Li et al. "Practical Implementation of an OPC UA TSN Communication Architecture for a Manufacturing System". In: *IEEE Access* 8 (2020).
- [74] Alberto Morato et al. "Assessment of Different OPC UA Implementations for Industrial IoT-Based Measurement Applications". In: *IEEE Transactions on Instrumentation and Measurement* 70 (2021).
- [75] Juan Wang and Di Li. "Adaptive Computing Optimization in Software-Defined Network-Based Industrial Internet of Things with Fog Computing". In: *Sensors* 18.8 (Aug. 2018).
- [76] Chuan Lin et al. "DTE-SDN: A Dynamic Traffic Engineering Engine for Delay-Sensitive Transfer". In: *IEEE Internet of Things Journal* 5.6 (Dec. 2018).
- [77] Peng Zeng et al. "Time-slotted software-defined Industrial Ethernet for real-time Quality of Service in Industry 4.0". In: *Future Generation Computer Systems* 99 (2019).
- [78] Sebastian Schriegel and Jürgen Jasperneite. "A Migration Strategy for Profinet Toward Ethernet TSN-Based Field-Level Communication: An Approach to Accelerate the Adoption of Converged IT/OT Communication". In: *IEEE Industrial Electronics Magazine* 15.4 (Dec. 2021).
- [79] Daniel Bujosa et al. "HERMES: Heuristic Multi-queue Scheduler for TSN Time-Triggered Traffic with Zero Reception Jitter Capabilities". In: *Proceedings of the 30th International Conference on Real-Time Networks and Systems*. 2022.
- [80] Pierre-Julien Chaine et al. "Egress-TT Configurations for TSN Networks". In: *Proceedings of the 30th International Conference on Real-Time Networks and Systems*. 2022.
- [81] Dietmar Bruckner et al. "An introduction to OPC UA TSN for industrial communication systems". In: *Proceedings of the IEEE* 107.6 (2019).
- [82] Tanushree Agarwal et al. "Multi-Level Time-Sensitive Networking (TSN) Using the Data Distribution Services (DDS) for Synchronized Three-Phase Measurement Data Transfer". In: *IEEE Access* 7 (2019).
- [83] Dave Cavalcanti et al. "Extending accurate time distribution and timeliness capabilities over the air to enable future wireless industrial automation systems". In: *Proceedings of the IEEE* 107.6 (2019).
- [84] Susruth Sudhakaran et al. "Enabling QoS for Collaborative Robotics Applications with Wireless TSN". In: *International Conference on Communications Workshops (ICC Workshops)*. IEEE, June 2021.
- [85] Zelin Yun et al. "RT-WiFi on Software-Defined Radio: Design and Implementation". In: *28th Real-Time and Embedded Technology and Applications Symposium (RTAS)*. IEEE. 2022.
- [86] Jaspreet Singh Walia et al. "5G network slicing strategies for a smart factory". In: *IEEE Computers in Industry* 111 (Oct. 2019).
- [87] Adnan Ajaz. "Private 5G: The Future of Industrial Wireless". In: *IEEE Industrial Electronics Magazine* 14.4 (Dec. 2020).
- [88] Miaowen Wen et al. "Private 5G Networks: Concepts, Architectures, and Research Landscape". In: *IEEE Journal of Selected Topics in Signal Processing* 16.1 (Jan. 2022).
- [89] Ilja Behnke et al. "Towards a real-time IoT: Approaches for incoming packet processing in cyber-physical systems". In: *Journal of Systems Architecture* (May 2023).
- [90] Ilja Behnke et al. "A priority-aware multiqueue nic design for real-time iot devices". In: *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*. ACM, 2022.
- [91] Bjarne Johansson et al. "Priority Based Ethernet Handling in Real-Time End System with Ethernet Controller Filtering". In: *IECON 2022–48th Annual Conference of the IEEE Industrial Electronics Society*. IEEE. 2022.
- [92] Henrik Austad et al. "Composable distributed real-time systems with deterministic network channels". In: *Journal of Systems Architecture* 137 (2023).
- [93] Yi-Hung Wei et al. "RT-WiFi: Real-time high-speed communication protocol for wireless cyber-physical control applications". In: *34th Real-Time Systems Symposium*. IEEE. 2013.
- [94] Shiva Raj Pokhrel et al. "Towards Enabling Critical mMTC: A Review of URLLC Within mMTC". In: *IEEE Access* 8 (2020).
- [95] Christoph Blumschein et al. "Differentiating Network Flows for Priority-Aware Scheduling of Incoming Packets in Real-Time IoT Systems". In: *International Symposium on Real-Time Distributed Computing*. IEEE, 2022.
- [96] Hansong Xu et al. "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective". In: *IEEE Access* 6 (2018).
- [97] Beom-Su Kim et al. "A survey on real-time communications in wireless sensor networks". In: *Wireless communications and mobile computing* 2017 () .
- [98] Emiliano Sisinni et al. "Industrial internet of things: Challenges, opportunities, and directions". In: *IEEE transactions on industrial informatics* 14.11 (2018).
- [99] Pangun Park et al. "Wireless Network Design for Control Systems: A Survey". In: *IEEE Communications Surveys & Tutorials* 20.2 (2018).
- [100] Claudio Zunino et al. "Factory Communications at the Dawn of the Fourth Industrial Revolution". In: *Computer Standards & Interfaces* 71 (Aug. 2020).
- [101] Kwang-Cheng Chen et al. "Wireless Networked Multirobot Systems in Smart Factories". In: *Proceedings of the IEEE* 109.4 (Apr. 2021).