Factory Communications at the Dawn of the Fourth Industrial Revolution

Claudio Zunino (a), Adriano Valenzano (b), Roman Obermaisser (c), Stig Petersen (d)
(a) CNR-IEIIT, C.so Duca degli Abruzzi 24, Italy
(b) (CNR-IEIIT), Italy
(c) (University of Siegen), Germany
(d) (SINTEF Digital), Norway

Abstract

The fourth industrial revolution (Industry 4.0) and its requirements impose radical changes to the underlying networking technologies that will be adopted in future factories. Most popular solutions in use today, in fact, are suitable for Industry 4.0 only in part, and new techniques and devices have to be developed to cope with demanding needs in terms of flexibility, communication bandwidth, real-time behavior, mobility, scalability, energy efficiency, reliability, availability and security. The goal of this paper is assessing the current situation of factory communication systems in the light of their evolution to support Industry 4.0 applications. The paper provides an overview of fundamental concepts in factory communication systems focusing, in particular, on prevalent wireless and wirebound communication protocols and standards. Research challenges in next generation industrial networks are also taken into account.

Keywords: Factory communication systems (FCS), industrial Ethernet, industrial wireless communications, distributed synchronization, localization, cybersecurity, Industry 4.0, industrial Internet of Things (IIoT), Smart Factory, software-defined networking (SDN).

1. Introduction

There is a general agreement in the scientific community of developed countries that maintaining industrial competitiveness means being able to deal with a great variety and high customization of products, very short time-to-market and shortened life cycles for goods. To address these challenges, manufacturing industries are adopting different strategies and advanced technologies, in

particular referred to as Industry 4.0 [1], Internet of Things (IoT) [2] and Industrial IoT (IIoT) [3], just to mention a few of them. This implies a progressive shift from traditional production control and automation systems to intelligent solutions, able to dynamically support rapidly changing and highly flexible production environments, so as to satisfy different processing requirements.

The fourth industrial revolution (Industry 4.0), in particular, is intended as an ambitious comprehensive approach to the ever increasing demand for unprecedented diversification of products, in order to achieve competitive advantages through radical changes in automation and flexibility of plants (it is worth remembering that, roughly speaking, the word "plant" is generally used to mean areas and/or buildings where something is processed (i.e. thermal power plants, petroleum refineries), while "factory" is adopted for places where something is manufactured and produced, although situations exist where both are present (i.e. drugs production with a wet processing phase and a dry pill production end). In the following, however, we will not care about this distinction and use the two terms interchangeably. Industry 4.0 implies a strong convergence of information (IT) and operation (OT) technologies, that is the integration of IT systems used for data-centric computing with OT systems to monitor and control events and processes, thus paving the way to completely new intra- and inter-enterprise architectures. This leads to completely new scenarios and affects a lot of social, economic and technical aspects that will heavily depend on the development and availability of adequate technologies, including the information and communication technology (ICT) domain [4]. A typical example is the evolution of human-machine interactions in collaborative robotics which significantly impacts on safety and demands for stringent real-time and reliability guarantees for active collision prevention/avoidance [5].

ICT solutions adopted in today factories are based on wired networks to support distributed industrial controls (e.g., specialized fieldbuses and Industrial Ethernet communications [6]). However, rewiring and reconfiguration are neither flexible nor inexpensive, so that wireless approaches are preferable in evolved manufacturing environments, where a large number of complex and

heterogeneous tasks and processes need frequent adjustments likely in real-time. This is why wireless communications are being considered as one of the most appealing technologies for perspective industrial applications.

Another key issue is the ability to cope with growing real-time needs in an effective and reliable way. New dependable and real-time capable solutions have then to be developed, which can address the timing and reliability requirements of Industry 4.0 for local and wide area networks (LANs and WANs).

Moving communication management functions from hardware to software is the approach followed by Software Defined Networking (SDN) [7] and Network Function Virtualization (NFV) [8] to enhance flexibility and to decouple traffic control from message filtering and forwarding. Actually, the main idea, in this case, is separating the data and control planes. While the former is kept inside forwarding devices, the latter is assigned to a central controller where the behavior of the whole network is managed in software.

The pervading interconnection of devices in IIoT and the expected increase of machine-to-machine (M2M) communications in a worldwide open scenario, also push for adequate protection methodologies and mechanisms to defend industrial networks from threats and menaces carried out through the cyberspace [9].

The Industry 4.0 scenario involves a large community of researchers, professionals and practictioners with advanced knowledge in several technological areas such as manufacturing, production, communication and information engineering. These people will be collectively referred to as "experts" in the following of this paper. They all agree that several aspects are likely to impact on digital networks in future industrial environments, however the goal of this paper is to focus especially on wireless and real-time communications, SDN and cybersecurity, to analyze how they can affect emerging technologies in the years to come.

The remaining sections discuss the emerging trends in some main areas of industrial communication research. With respect to other surveys that have appeared in the literature, we follow a more comprehensive approach, taking into consid-

eration different industrial network technologies instead of focusing on specific types of solution.

In particular, the paper is structured as follows: Section 2 briefly summarizes some significant related works appeared in the literature. Section 3 recalls most popular communication solutions in use in recent years, while Section 4 introduces some main goals of Industry 4.0 that communication technologies may contribute to achieve. Section 5 deals with challenges pertaining to the ICT domain that have to be tackled in industrial systems, summarizing how technologies already in use can start, at least in part, to satisfy the increasing demand in terms of openness, reliability, real-time capabilities and flexibility. Section 6 briefly discusses the main characteristics of some promising and emerging technological solutions, and Section 7 draws some conclusions.

For the reader's convenience acronyms used throughout this paper are listed in Table 1 with their associated meanings.

2. Related works

A theoretical analysis for state estimation, determination of closed-loop stability and controller synthesis when sensors and actuators communicate with a remote controller over a multi-purpose network has been carried out in [10]. The survey addresses several key issues such as packet-rates, sampling, network delay, and packet dropouts. Some comprehensive studies on communication network in industrial environments are presented in [11], [6] and [12].

These papers focus on trends in the first decade of 2000s and show how solutions evolving from fieldbuses and industrial Ethernet to wireless and Internet-based networking made their appearance and introduced new issues about standardization and dependability.

The adoption of wireless communications in industrial application was dealt with in [13], where both IEEE 802.11 and Wireless Sensor Network (WSN) technologies were analyzed in order to evaluate their suitability for industrial environment. In [14], a WSN-oriented discussion is presented. Authors divide industrial application domains into classes with similar needs, then consider

Table 1: Acronyms and meanings

Acr.	Definition	Acr.	Definition
5G	Fifth Generation (mobile networks)	NETCONF	Network Configuration (Protocol)
AI	Artificial Intelligence	NFV	Network Function Virtualization
API	Application Programming Interface	NoN	Network of Networks
COTS	Commercial-Off-The-Shelf	LAN	Local Area Network
CPS	Cyber-Physical System	OCSVM	One-Class Support Vector Machine
CySeMoL	Cyber Security Modeling Language	PAN	Personal Area Network
DetNet	Deterministic Networking (Working Group)	PLC	Programmable Logic Controller
DiffServ	Differentiated Services	PRM	Probabilistic Relational Model
DMZ	Demilitarized Zones	PRTS	Pareto Reactive Tabu Search
EFP	Extra-Functional Property	PSA	Pareto Simulating Annealing
ERP	Enterprise Resource Planning	QoS	Quality of Service
FDMA	Frequency Division Multiple Access	RBAC	Role-Based Access Control
FW	Firewall	RSP	Random Search Pareto
ICS	Industrial Control System	RTE	Real-Time Ethernet
ICT	Information and Communication Technology	SAE	Society of Automotive Engineers
IE	Industrial Ethernet	SCADA	Supervisory Control And Data Acquisition
IIoT	Industrial Internet of Things	SDMA	Space Division Multiple Access
IoT	Internet of Things	SDN	Software Defined Networking
M2M	Machine-To-Machine	TDMA	Time-Division Multiple-Access
MAC	Medium Access Control	TSH	Tri-criteria Scheduling Heuristic
MC	Mixed-Criticality	TSN	Time Sensitive Networking
MES	Manufacturing Execution System	TT	Time-Triggered
MIP	Mixed-Integer Programming	TTE	Time Triggered Ethernet
MPLS	Multiprotocol Label Switching	WAN	Wide Area Network
MPSoCs	Multi-Processor Systems-on-a-Chip	WSN	Wireless Sensor Network

and evaluate representative protocols with respect to their specific functions addressing the class requirements. Security features are also taken briefly into account.

A general analysis on machine-to-machine communication is carried out in [15], where authors discuss different issues on the roles of M2M communications in perspective ultra-dense networks. More specifically, they focus on the implementation of M2M communications by reasoning on four-layered architectures, including the physical, media access control (MAC), network, and application

layers.

In [16] the authors offer a comprehensive survey of research activities in IIoT. They describe architectures, applications and their main characteristics in recent research efforts from three key viewpoints, that is control, networking, and computing. In particular, a framework is proposed to explore the research space in the communication area and an investigation on some representative networking technologies, including 5G, M2M communication and SDN is presented.

Finally, a survey on Industrial Internet is found in [17], with particular attention to architectures, enabling technologies, applications and technical challenges. The paper first introduces the history of Industrial Internet, then presents a five-level architecture typically adopted to describe Industrial Internet systems. In addition, this contribution also describes how application domains like energy, health care, manufacturing, public section, and transportation are being gradually transformed by Industrial Internet technologies.

3. Factory communications between past and present

From a historical perspective, the first and second industrial revolutions (see Fig. 1) leveraged steam power and mechanization, then electricity and assembly lines, to increase production and efficiency. In the seventies, the third revolution started an ever increasing adoption of electronics in factories and products. This also marked the beginning of a new epoch where device communications (initially analog then digital) gained progressively importance.

Most typical and widespread digital networking solutions in vintage automation were based on specialized fieldbuses that can be considered as the first generation of industrial networks [18]. Though fieldbuses are rather obsolete today, their use is still widespread and some (enhanced) field communication technologies are indubitably popular (e.g., automotive industry) and maintained either for compatibility reasons or special-purpose applications. The diffusion of fieldbuses installations was slowed down and practically halted because of the maturity level reached by several Ethernet-based solutions offering devices and

applications especially conceived for factory and automation environments. This second generation of industrial networks is also known as Industrial Ethernet (IE) or Real-Time Ethernet (RTE) [19].

Indeed, with respect to the well-known automation layered architecture, compliant to the ISA 95 pyramidal model shown in Fig. 2, main research challenges with fieldbuses were granting interoperability and allowing internetworking of different automation layers while preserving the real-time communication capabilities of field networks. Ethernet-based and TCP/IP LANs were usually employed at the control and process management levels [11], thus the need for integration pushed for adopting Ethernet also at the field level, so as to take full advantage of uniform network architectures and protocols. Unfortunately, standard Ethernet, which is mainly oriented to office and business applications, is often unsuitable for factory automation or process control. Consequently, a family of Ethernet-based protocols had to be studied and developed for shopfloor communications, that adopt most Ethernet techniques and mechanisms at the physical and datalink communication levels, but cannot be completely compatible with conventional Ethernet devices. Real-time Ethernet solutions such as PROFINET [20], Ethernet POWERLINK [21], EtherCAT [22] and others, belong to this class of industry-oriented protocols and enable the separation of normal and real-time traffics, for instance by introducing changes in the standard medium access control (MAC) layers to support prioritization or time-division multiple-access (TDMA) schemes. A typical scenario could be a network consisting of Ethernet standard components for connection to PLCs and an RT-Ethernet subnetwork between PLCs and I/O devices, adopting some modified version of the Ethernet protocol. Software- and hardware-based solutions were developed to satisfy real-time requirements, with the latter enabling, in general, shorter response times and lower jitters. Protocols such as Time-Triggered Ethernet (TTE) were made available as either h/w or s/w implementations, implying differences in temporal properties such as the precision of the global time base or the communication jitter [23]. In some particular situations, however, ad-hoc solutions had to be developed which are based on

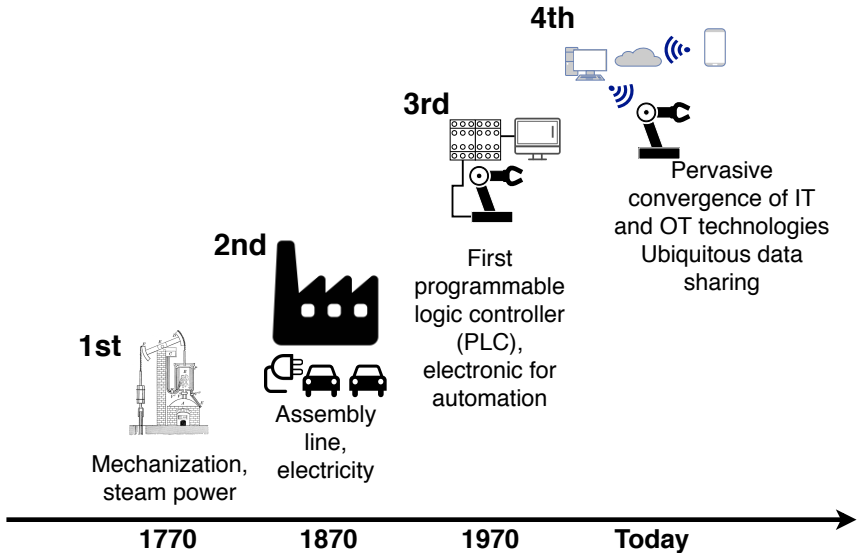

Figure 1: The four industrial revolutions.

application-specific integrated circuits (ASIC) and this augmented the importance of Systems-on-a-Chip (SoC) with Intellectual Property cores for real-time Ethernet (e.g., LS1028A Soc of NXP with TSN).

One of the main novelties in industrial communication in the last decade is the introduction of wireless technologies in the fields of factory and process automation. Initiated by the emergence of the IEEE 802.11 family of standards [24] for high capacity wireless LAN connections, and the Bluetooth specifications [25] for simple connectivity for personal area networks (PANs), both open and (typically) proprietary solutions based on these approaches have started to be considered for use in plants and factories too. However, while the high capacity IEEE 802.11 is ideal for some application areas, the relatively high power consumption makes it unsuitable for battery-powered operations.

By contrast, the relatively short range allowed by Bluetooth, combined with the difficulties to support different topologies beyond simple piconets and scatternets, makes it typically unsuitable for large networks connecting more than a single factory cell. Moreover, although the last version of the specifications

also includes mesh topologies [26], [27], to the best of our knowledge, only home/office-oriented devices have started to appear on the market.

These drawbacks have paved the way to proposals for wireless field instruments, defined as a merger of wireless sensor network (WSN) technologies with factory and process automation disciplines. Wireless instrumentation has become increasingly popular in factories and process industries after the ratifications of the WirelessHART [28], ISA100.11a [29] and WIA-PA [30] specifications. By providing reliable self-healing and self-configuring wireless communication, these standards offer cost-efficient alternatives to wired field instruments [31]. Wireless field instruments are typically traditional, formerly wired, sensors and/or actuators equipped with additional radio transmitters, antennas and power supplies (batteries). The instrument parts (i.e. sensor or actuator elements) are usually the same as for their wired counterparts, thus they have comparable measurement performance and accuracy characteristics.

For automation disciplines, wireless instrumentation is the third evolutionary stage in the field device communication technology. In fact, in the first historical stage each field instrument required a dedicated cable linking the device directly to the control system. Fieldbus solutions, in the second stage, allowed to reduce the cabling complexity thanks to a single shared wire, connecting the controller to all field devices. Finally, the recent introduction of wireless instrumentation has enabled field devices to get rid of cables, through radio connections to wireless access points. Wireless networks are configured, managed and controlled by network managers, which are typically separate devices connected to the backbone plant (industrial Ethernet) network [32].

Initially, wireless instrumentation was exclusively used for non-critical monitoring tasks, measuring slowly changing parameters such as temperature and pressure but, with the evolution of technology, application areas were progressively extended to perform more sophisticated supervision functions (e.g., vibration [33] and sound [34]), or included in safety-critical applications (e.g., gas detection [35]). Hybrid approaches were also adopted, with wireless subnetworks connected to either a backbone or a LAN [36], [37], [38].

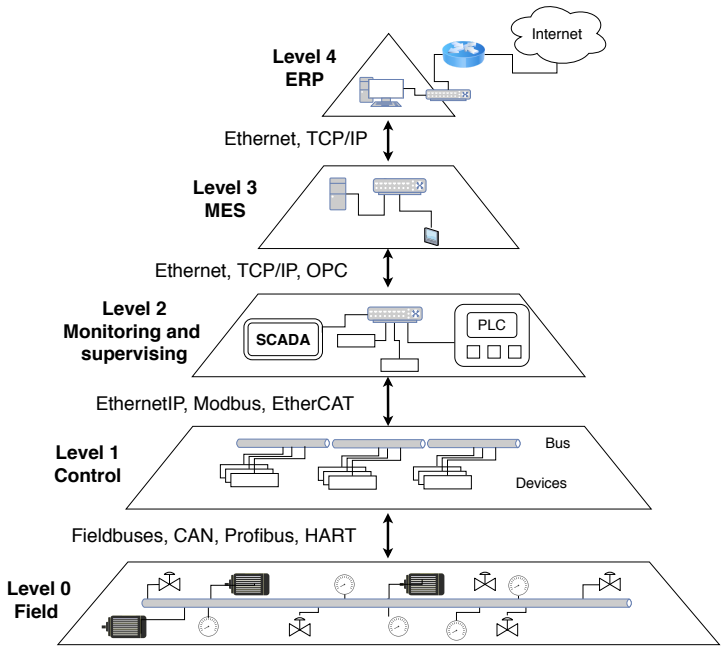

Figure 2: Traditional organization of automation systems.

As a matter of facts, however, the automation pyramid in Fig. 2 is still the reference model for a large number of existing industrial scenarios, because of delays and a certain degree of inertia in introducing changes and replacing well-assessed (but also aging) technologies. This, of course, has an impact on communications too. It is well known that the model layers (field, control, process management and enterprise) play roles of separate, cooperating entities. At the lowest level signals are exchanged between sensors/actuators and their controllers (i.e. PLCs). Scalability and reconfiguration are major issues here, especially considering the dramatic increase in the number of connected devices expected for next-generation automation. Unfortunately, besides horizontal connections, vertical integration [39] has to be taken into account carefully. Actually, the traditional pyramidal organization in Fig. 2 imposes rigid constraints on communication as any layer can exchange information only with its adjacent neighbors. This limitation has to be overcome in Industry 4.0 as,

in principle, all data should be shared and made readily available to any entity in the distributed system, independently of their physical locations. To prevent this, Industry 4.0 technologies and paradigms have to be conceived in order to provide adequate support for transferring and processing huge amounts of information in an end-to-end fashion.

In evolved automation, production lines and manufacturing processes are expected to be more compact and modular, but also able to effectively establish direct connections (either physical or logical) to share information whatever needed. This means that the hierarchical model in Fig. 2 must be replaced with a new architecture, whose advanced network infrastructure is no longer binded to a layered organization but enables direct end-to-end communications by leveraging cloud/internet services as shown in Fig. 3. The figure conveys the idea that the five layers (and devices belonging to them) are no longer connected in a cascaded fashion, but they are able to communicate end-to-end through the cloud/internet infrastructure. Actually, modular solutions, by their nature, allow to shorten the time for installation and setup, while the system operation and maintenance are simplified. Benefits of modularity are in fact clear: for instance, in case of repair, shutting down a single component rather than putting a whole production line offline makes the difference. And as the market increases its demand for modular and flexible systems, the availability of dynamic, plug-and-produce infrastructures based on advanced communication architectures become more and more important.

4. Industry 4.0 and Factory Communications

From the Industry 4.0 viewpoint, increasing competitiveness through the enhancement and customization of products also means introducing a number of structural changes in today production systems. In particular, the organization of factories and plants are expected to move from the currently adopted "push to the market" approach to innovative "pull from the customer" solutions. This leads to the adoption of new strategies able to combine the needs for final prod-

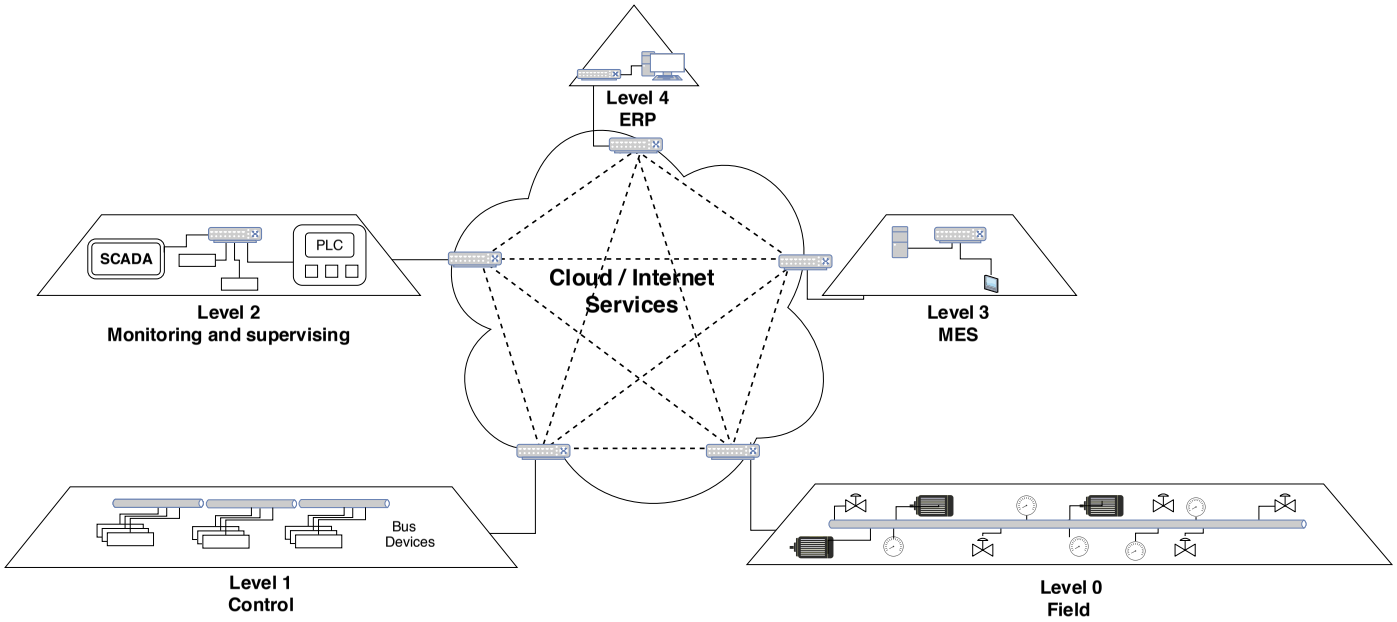

Figure 3: Automation layers interconnection in Industry 4.0.

ucts, which are totally customized according to individual consumer's desire, with the typical requirements of mass production techniques, though taking advantage of high flexibility and fast reconfigurability.

Interoperability is another key concept which is frequently mentioned together with flexibility in perspective Industry 4.0 scenarios. In practice, manufacturing systems and their components (i.e., work-piece carriers, assembly stations and even products themselves) have to share and exchange information autonomously, while smart factories, devices and humans should be able to establish connections and communicate thanks to the fundamental role played by the ICT ubiquitous infrastructure [40]. Communication technologies are then going to become key enablers for both vertical integration of smart (custom-specific) production systems and horizontal integration of innovative production chains (e.g., supplier-manufacturer-customer revisited) allowing the development of innovative business and cooperation models.

Clearly, ICT cannot grant the achievement of all these goals on its own as many other social, economic and policy-dependent aspects should be considered, that are not in the technological scope. However, ICT is responsible for providing adequate answers to the even exasperated demands for flexibility, reconfigurability and interoperability and offering advanced solutions where conventional approaches in use today prove to be unsatisfactory [41].

In a general overview, smart factories, which are based on cyber-physical production systems (CPPSs), rely on smart machines. Actually, smart machines are not that far from advanced solutions already in use in modern factories, provided they are enabled to share information about materials, requests for production changes, faults, stock amounts and so on. Thus, research activities are investigating some main problems concerning, in particular:

- the availability of ultra large communication bandwidth to support the exchange of huge amounts of data in real-time (i.e. for predictive maintenance [42]);
- the security of communications and protection against attacks and un-

wanted (malicious) behavior in a global scenario where billions of devices can dynamically connect and cooperate without human intervention/supervision [43];

- the augmented resilience of networks to grant normal operation with constant levels of quality of service (QoS), even in critical conditions because of misconfigurations, faults and/or attacks [44];
- the scalability of future networks to accommodate the exponential growth of connections and dynamically changing demand for QoS [45];
- the predictability of links and connections to enable easy adaptation to quickly changing needs and working situations [46].
- the real-time communication support to enable a strong enterprise-control systems integration, where factory control and supervisions are tailored to small production batches even on customer's demand [47].

Though the availability of solutions to these scientific issues is not enough to provide all the expected Industry 4.0 benefits, experts agree that they can help with the development of a new generation of powerful smart communication networks.

In a wider scenario, smart factories should be able to interface and cooperate with other smart environments such as smart grids, smart buildings/homes and take advantage of smart logistics and mobility services. At the same time they are expected to enable an extensive merge of real and virtual environments and deeply change production systems consequently. New challenges are then appearing in the scientific arena and some open issues are:

- **network self-awareness**, and, in particular, the ability to dynamically adjust the operating parameters autonomously, according to changing user requirements and/or environmental conditions [48];
- **network self-management** and, in particular, the ability to analyze, identify and fix problems without human intervention [49];

- **network self-healing**, and, in particular, the ability to perform self-reconfigurations when faults occur, leveraging redundant resources and intelligent algorithms [50].

The reader must be warned that, to the best of our knowledge, these challenging aspects have started being debated in the scientific community, but neither detailed technical contributions have appeared in the literature so far, nor mechanisms and support are included in off-the-shelf products and solutions ready for large-scale deployment. Ongoing studies in these directions are likely to find answers and results from the artificial intelligence (AI), automated learning and knowledge management research areas.

5. Factory communications and technology challenges

A number of technologies already in use in today factory communications look if not completely adequate, at least a good starting point to move towards the expected Industry 4.0 scenario. In particular, in this paper we focus on their ability to fulfill a set of fundamental requirements including **openness**, **real-time**, **security**, **reliability** and **scalability** [51].

Indeed, several investigations appeared in the literature focus on easing the inter-operation of machines, robots, sensors and logistic systems via a hierarchy of private/public networks and the Internet [52]. Thus, openness has progressively emerged in the scientific community as a main viable solution and become a mandatory key concept to enable the integration at run-time of new components, in order to dynamically implement emerging global services.

Similarly, support for reliable operation [53] and hard real-time communication [54] are deemed more and more fundamental to enable closed-loop control and guaranteed response times. Examples of reference scenarios, in this case, are remote maintenance applications and optimized production processes. In perspective, new dependable and real-time capable solutions are required to support the RT- and reliability-eager applications of Industry 4.0 for both lo-

cal and wide area networks. Standardization has also started moving to this direction: for instance, the Deterministic Networking Working Group (DetNet) [55] is focusing on deterministic paths over layer 2-bridged and layer 3-routed network segments.

Another main challenge for future open and dynamic system architectures is the modeling of information and consideration of semantics in the dynamic composition of services. Ongoing activities for standardization of real-time capable OPC UA [56] is a serious attempt to satisfy stricter requirements for interoperability and information modeling with hard real-time needs.

5.1. Mixed-Criticality Systems

An increasing trend to adopt so-called mixed-criticality (MC) systems can be observed in many application domains such as avionics, industrial control and health-care, where multiple functions with different degrees of importance and certification assurance levels are integrated using a shared computing platform. This area is going to receive particular interest by the scientific community in the near future, as embedded systems and applications are already becoming more and more pervasive and will be extremely popular in tomorrow IIoT. MC is the concept of allowing applications at different levels of criticality to seamlessly interact and co-exist on the same networked computing platform. Foundations of this integration are mechanisms for temporal and spatial partitioning, which establish fault confinement and the absence of unintended side-effects between functions. Partitions encapsulate resources temporally (e.g., latency, jitter, duration of availability during a scheduled access) and spatially (e.g., prevent functions from altering code or private data of other partitions).

There is also evidence of significant orientation for innovative solutions adopting Multi-Processor Systems-on-a-Chip (MPSoC) components in embedded systems deployed in industrial applications and, in this framework, up to 95% of MPSoC devices is expected to combine cores of mixed-criticality levels [57]. By contrast, the latest processor generations for use in industry are equipped with

multiple cores, but typically only one of them is actually devoted to highly-critical tasks [58]. This misuse or reduced utilization is due to several technical reasons such as the need to prevent delays in concurrent cache accesses by different cores, but also to the lack of adequate breakthroughs in the area of multicore real-time operating systems [59], [60]. Moreover, even though solutions for temporal and spatial partitioning in multi-core processors have started to appear, some main technological problems at the chip level are yet far from being solved. These include, for instance, the combination of software virtualization and hardware segregation and the extension of partitioning mechanisms to jointly satisfy extra functional requirements (e.g., time, energy and power budgets, reliability, safety and security).

5.2. Reliable and Deterministic Wide-Area Communications

Industry 4.0 requires the interconnection of geographically dispersed computer systems to make smart machines able to share information at each stage of the production chain and obtain full horizontal and vertical integration in a totally distributed fashion. This motivates the increasing attention of researchers towards reliable wide-area communication solutions across multiple network domains [61].

To achieve effective real-time exchanges of critical data between remote constituent systems, IP-based mechanisms have to be suitably expanded so as to support dependable and temporally predictable inter-domain traffic management. At present, network administrators are able to deploy QoS-aware mechanisms in their administrative domains to handle different types of network traffic (typical examples are the Multiprotocol Label Switching (MPLS) [62] and the Differentiated Services (DiffServ) [63] techniques), but this is not enough in perspective. A first attempt to deal with dependability and timeliness in multi-domain traffic has been presented in [64], [65]. However, complementing the traditional IP technologies for QoS assurance to include reliability and determinism is an ambitious goal that involves significant research and experimentation effort in the next years.

The Deterministic Networking initiative [66] mentioned previously focuses on deterministic data paths over layer 2-bridged and layer 3-routed segments, to offer bounded latency, packet losses and packet delay variations (jitters) as well as guarantees about reliability.

5.3. Combination of Real-Time and Extra-Functional Requirements including Security, Reliability and Scalability

Frequently factory communication systems have to support hard real-time control applications, where the stability and safety of the control action depend on activities such as sensor data acquisition, command computation and transmission to actuators in bounded time. In such conditions, missed deadlines are system failures which can have consequences as serious as in the case of providing incorrect results. As deterministic response times have to be guaranteed even in the case of peak load and fault scenarios, timing and resource analyses are used to assess the worst-case behavior of the system in terms of communication delays, computational delays, jitter, end-to-end delays and temporal interference between different activities. Factory communication technologies have then to be conceived so as to ensure determinism and low jitter (i.e., difference between maximum and minimum computational and communication delays). Indeed, control algorithms can often be designed to compensate known delays, but jitters introduce additional (and sometimes unknown) uncertainty into the control loops, so that suitable mechanisms have to be provided to keep such a kind of variations as small as possible. This aspect has already been considered for some protocols in use today [67], [68] but it is going to receive increasing attention in future factory networks.

Besides real-time requirements, additional extra-functional properties (EFPs) such as reliability, energy-efficiency and scalability have to be taken into account to achieve acceptable behavioral trade-offs [69]. For example, a system designed for best performance could easily involve high power consumption, while an optimal solution from the reliability point of view might be unsatisfactory in terms of latency. Actually, one main problem in the design of both present and next

generation networks is finding adequate approaches which are able to combine performance and EFPs. Multi-criteria optimization techniques can be adopted in fine-tuning EFPs and get the best trade-offs, for instance through exploration of points in the Pareto curve [70]. The curve is used to select the best value for a given property under constraints imposed by other properties. In this way, for example, the reduction of power consumption can be evaluated under performance constraints by exploring the points in the design space. As an exhaustive search is often unfeasible because of the space size, numerous methods have been suggested to speedup the exploration process. In [71] the authors proposed an optimization structure to estimate the Pareto curve without delving into the whole design space. An extension to that technique was then presented in [72], by integrating genetic algorithm analysis for dependent parameters optimization. The work presented in [73] exploited heuristic algorithms analysis (namely, Random Search Pareto (RSP), Pareto Simulating Annealing (PSA) and Pareto Reactive Tabu Search (PRTS)) to explore the design space and find the Pareto curve for EFPs in a short time. Obtained results showed that an approximate Pareto curve can be estimated three orders of magnitude faster than a full search.

Finally, a Tri-criteria Scheduling Heuristic (TSH) was developed in [74] which is able to combine timing, reliability and power-consumption requirements to produce a static schedule starting from a software application graph and multiprocessor architecture.

5.4. Industrial wireless communications

The advantages of adopting wireless communications in current factory networks are manifold. Most obvious business drivers concern cost savings from simplified engineering, commissioning and installation, because of the elimination of cables. In addition, wireless sensors and actuators offer ease of modifications and replacements due to reduced work complexity. They also enable fast and simple introduction of temporary instrumentation, besides allowing the use of more mobile and portable field equipment during maintenance, setup and

tuning operations. [31].

Besides these benefits already achievable today, however, the increasing needs for communication capacity foreseen by IIoT and Industry 4.0 demand more and more to industrial wireless systems. This includes the ability to handle many more connected devices and data to transmit at a higher update rates than current solutions [61]. Wireless sensor networks currently in use (e.g., WirelessHART, ISA100.11a and WIA-PA) were originally conceived for low-power and high reliability communication in medium-sized networks, characterized by low to moderate data rates [75]. The expected increase, both in the number of devices per network and update rate per device, can hardly be managed with those technologies, especially when network capacity and battery lifetime have also to be taken into account, so that new solutions have to be studied and developed. A possible solution to enable soft RT communication in wireless IEEE 802.11 environments has been proposed in [76]. The RT-WiFi architecture, which is able to handle together both non-RT and RT traffic, combines a forcing collision resolution MAC that prioritises RT traffic with a TDMA mechanism that serializes the access of RT stations to the communication medium.

5.4.1. Network capacity

WirelessHART, ISA100.11a and WIA-PA inherit their physical layers from IEEE 802.15.4, and employ a combination of TDMA and frequency division multiple access (FDMA) as medium access mechanisms [32]. Communication is structured into distinct timeslots with a typical duration of 10 ms. A collection of timeslots forms a superframe which is transmitted repeatedly in time throughout the network operation. The transmission of at least one superframe must always be enabled, though multiple superframes of variable lengths can coexist in the network. Superframe schedules can be added and removed while the network is operated. Transmissions are managed by assigning two devices to each timeslot, acting as source (transmitter) and destination (receiver) respectively. Broadcast messages are exceptions as multiple devices play the role of receivers in the same timeslot. TDMA allows for deterministic communication,

while FDMA grants robustness against localized noise and interference, however both these strategies are prone to scalability issues as the number of devices and the number of links in the network increases. For this reason, improved WSNs have to support a growing number of links with unambiguous placements in the superframe, while for large networks the size of the superframe has also to be enlarged, despite this increases the overall latency. Similarly, devices with high update rates require shorter interval between consecutive timeslots and this contributes to put serious constraints on the network capacity. Solutions to these problems have started to be studied such as the one in [77], which combines a TDMA approach with relaying and packet aggregation.

When a larger communication bandwidth is needed, techniques inspired by the IEEE 802.11 standard and its evolution look promising. For example, [78] presents a theoretical analysis and experimental evaluation of IEEE 802.11n to identify recommendations for its effective use in real-time industrial networks. The enhancement of reliability for industrial wireless transmissions by means of seamless redundancy is dealt with and evaluated in [79]. Finally, an innovative approach is presented in [80], which combines retransmission scheduling, seamless channel redundancy and bandwidth management to improve the determinism in wireless networks and support soft real-time industrial applications.

5.4.2. Battery lifetime

The key benefit of cable elimination also involves having batteries as power sources but, unfortunately, batteries are subject to periodic replacements in the field as they are expended. Battery lifetime for wireless field devices is one of the main limiting factors for their financially viable deployment, as the cost reductions have to be evaluated by taking into account the increased maintenance cost for battery replacements [31]. Battery lifetime for wireless field instruments is highly dependent on the update rate, as radio transmissions and sensor measurements are two elements with the highest power consumption [81]. The expected increase of sensor data update rates in IIoT and Industry 4.0 implies a growth of power consumption by wireless field devices. For these reasons,

Table 2: Emerging technologies and relevant network characteristics

Requirements	**Technologies**	**Improved Characteristics**	**Relevant Research Contributions**
Communication bandwidth	5G and optical networks	throughput, latency, reliability, security	[88], [89], [90], [91], [92], [93], [94], [95], [96], [97]
Reliability	RT-networks and SDN	determinism, standardization, performance	[8], [98], [99], [67], [68], [69], [100], [101], [102], [103], [104],
Scalability and mobility	Wireless comm. & IIoT	energy efficiency, determinism, availability	[38], [48], [76], [77], [78], [79], [80], [82], [83], [85], [86], [87], [105], [106], [107], [108]
Security	Active/passive Cybersecurity	safety, availability, integrity, confidentiality	[109], [110], [111], [112], [113], [114], [115], [116]

several techniques have been proposed to save power, ranging from packet size optimization [82] to routing algorithms [83], so as to maintain a viable tradeoff between battery and performance in advanced networks. Nevertheless, these solutions have to be complemented with the investigation and development of more efficient wireless communication protocols and methods for energy harvesting [84] to grant satisfactory battery lifetime and communication performance in next generation (smart) networks too.

At present, some vendors offer products including circuits that are able to transform an RF signal in charging voltage and current. In [85], a detailed theoretical study was presented and literature surveyed to provide new ideas for research in the domain of radio frequency energy harvesting. Another approach, based on a thermal energy harvesting technique, is presented in [86] which leverages the Seebeck effect on a Peltier element placed in the proposed architecture. Then, a well-designed MAC protocol can manage accesses to the channel so as to use the harvested energy efficiently and maximize performance, as shown in [87].

Table 3: Comparison of main communication parameters

		Current			**Expected**
Wired	Network size (nodes)	10-1000			>10000
		Not RT	Soft RT	Hard RT	Isochronous
	Response Time	>100 ms	∼10 ms	1 ms	200 ns
	Jitter (% of Resp. Time)	∼100%	15%	1%	1%
	Bandwidth	100 Mbps-1 Gbps			400 Gbps
Wireless	Network size (nodes)	10-1000			>10000
	Tx.time + ACK	0.5-10 ms			20 ns
	Bandwidth	1 Mbps-6 Gbps			20-40 Gbps

6. Emerging technologies and perspective directions

There is a general consensus that demands for highly personalized customer requirements are likely to be satisfied through smart factories, where current production systems are replaced by so-called smart-boxes, that is modular, highly reconfigurable and re-usable (plug-and-produce) components. As these benefits cannot be achieved without massive exchanges of information and data (e.g., between the customers' desktop/mobile devices and the production plants) and direct and autonomous interactions between smart-boxes, more flexible and adaptable network solutions are necessary, that are able to tackle the critical aspects discussed previously. However, implementing the visionary scenario of Industry 4.0 is not easy because of the many technical challenges to be addressed. From the communication network point of view, it is clear that much better performance is needed in terms of communication bandwidth, latency, real-time behavior, security, reliability and mobility. This increase in basic requirements can be satisfied only partially by leveraging technologies available today.

Table 2 lists some priority needs and emerging solutions that are being proposed and experimented to cope with them. The table also summarizes those network characteristics that are expected to benefit from the proposed technical solutions and includes references to main scientific contributions in the relevant areas. Of course, all these aspects impact on Industry 4.0 strategic goals and,

in particular:

- **Bandwidth** directly affects the ability to support the interconnection and data exchange of a very large number of devices.
- **Reliability** affects the ability of performing consistently well, having the overall system working properly in any condition. Obviously, this aims at increasing productivity.
- **Scalability** enables the smooth introduction of new devices, services and functions, without negative effects on the quality of services and functionalities already deployed.
- **Security**, and in particular cybersecurity, is mandatory for Industry 4.0 global scenarios to protect people and assets from attacks and malicious behavior.
- **Mobility** is in strict connection with the ability to distribute services and goods dynamically and ubiquitously to users moving around.

To offer the reader a flavor of the improvements requested for next generation factory networks, Table 3 reports some typical communication parameter values for both wired ([117], [118]) and wireless solutions ([78], [119]).
Values in the middle column are frequently found in current applications and have to be compared to the (expected) figures in the rightmost column. Even by this limited comparison, the size of the existing gap is evident and explains why new approaches have to be mandatory identified and adopted.

In the following subsections benefits expected by emerging technologies in terms of the characteristics listed above are briefly discussed. Moreover, what is necessary in terms of security, a surely emerging topic, is reported in Section 6.4.

6.1. Industrial Ethernet Extensions

Advantages of introducing Ethernet-based technologies in factory networks include high bandwidth, open standard protocols based on IEEE 802.3 and low

costs for commercial-off-the-shelf (COTS) devices. Ethernet extensions proposed in the recent past (e.g., Ethernet POWERLINK [21], Sercos III [120], PROFINET IRT [20], Ethernet/IP [121], AFDX [122] TTEthernet (TTE) [123] and Time Sensitive Networking (TSN) [61]) are able to offer temporal guarantees and improved dependability, but they also provide reasonable basis for a smooth migration to evolved factory networks. It is worth remembering that Industrial Ethernet products have progressively established a 46% market share with a 22% yearly growth rate [124].

Current and near future demanding requirements for hard real-time and fault confinement in several application areas can be satisfied through the Time-Triggered (TT) extensions to conventional Ethernet. In TT networks, communication activities are controlled by the progression of a global time base. Each node sends messages with predefined periods and phases regardless of events occurring within the node and/or in the environment. TT networks are beneficial in safety-critical systems, because they help in managing the complexity of fault-tolerance and analytic dependability models. A static schedule (frequently adopted in TT systems) minimizes unpredictability, while dynamic scheduling (typically found in event-triggered networks) unfolds dynamically at runtime, depending on the occurrence of events. It is worth noting that dynamic scheduling can be used in TT systems too, even though this may introduce some limitations [104]. In a time-triggered network, the predetermined instants of the periodic message exchanges enable rigorous error detection and fault isolation. Redundancy can be provided transparently to applications, that is without changing function and timing of the application software. TT systems also support replica determinism, which is essential in establishing fault-tolerance through active redundancy. Furthermore, they enable temporal composability via a precise specification of interfaces between subsystems.

Time-Triggered Ethernet (TTE) [123] is perhaps the most popular commercial solution based on the TT paradigm. TTE services are standardized by the Society of Automotive Engineers (SAE) and concern fault-tolerant clock synchronization as well as communication. In addition, TTE supports the in-

tegration of time-triggered and event-triggered messages in the same physical Ethernet network.

6.1.1. Time Sensitive Networking (TSN)

Time-triggered Ethernet solutions are now converging towards a new IEEE standard known as TSN, which is gaining increasing importance in industrial scenarios and can influence the evolution of factory networks in the next years, due to its ability to achieve low transmission latency and high availability. Its main features include robust time synchronization protocols, time-based scheduling, traffic policing, frame preemption, fault-tolerance by frame duplication and configuration capabilities with the Network Configuration Protocol (NETCONF) [125]. In this framework, the IEEE 802.1Qbu Preemptive Priority Frame Forwarding [126] defines mechanisms to interrupt the transmission of a message in order to send other frames with higher priority. The IEEE 802.1CB Frame Replication and Elimination for Reliability technique [127], instead, supports the duplication of messages for improved reliability. Finally, stream filtering and policing are considered in IEEE 802.1Qci [128] to detect and contain message transmissions of individual end-nodes that could disrupt the correct behavior of the whole system.

As a matter of fact, Ethernet extensions for industrial applications are able to cope with the technological challenges introduced in Section 5 only partially. In particular, Real-time, reliability and determinism requirements can be satisfied only for closed systems (e.g., timing analysis using network calculus [129], trajectory approach [130]), whereas dynamic system structures with real-time needs are insufficiently addressed. By contrast, pilot works on plug-and-play in TSN are beginning to appear. In particular, [98] shows how to provide hard real-time guarantees, but that proposal is only applicable to a star-shaped network topology and is not supported by COTS devices. Existing solutions for dynamic scheduling in TTE offer timing guarantees, but limited scalability [99]. The deployment of new configurations is available in TSN via the NETCONF

protocol and related configuration languages [131]. Instead, mixed-criticality is supported by combining different traffic classes such as time-triggered, rate-constrained and best-effort communication in TTE and TSN. Last but not least, fault isolation for time/space partitioning and modular certification is achieved by leveraging a priori knowledge about the permitted temporal behavior of end-systems in both TTE and TSN stream filtering and policing.

6.2. Software-Defined Networking (SDN) and Network Virtualization (NFV)

The software-defined networking paradigm is promising to grant openness, reliability and flexibility. Indeed, SDN is a key technical solution which can enable dramatic changes in the way the network infrastructures, such as the one depicted in Fig. 4, have been conceived so far. Many of the technical and scientific issues concerning flexibility, reconfigurability and capabilities for self-adaptation and management may find either adequate answers with SDN or, at least, basic support and mechanisms to build more sophisticated smart network control and supervision architectures. Moreover, the rapidly emerging SDN technology looks suitable to enable the development of networks of smart machines based on evolving ICT systems.

First, SDN breaks the monolithic, traditional network architecture by separating the control logic (control plane) from the underlying traffic filtering and forwarding mechanisms (hard-wired in routers and switches) that build up the data plane. The SDN control plane is centralized and software-programmable as shown in Fig. 5. In this way routes for traffic flows can be configured and modified by a high-level network manager (e.g. SDN controller) according to dynamically changing needs. Second, because of the separation of control and data planes, network switches can be implemented as simple forwarding devices, where no hop-by-hop mechanism has to be provided since no routing decision has to be made any longer by intermediate nodes placed along a route. Decoupling of control and data planes is obtained thanks to a clearly-defined application programming interface (API) enabling the exchange of information between the SDN controller and the switches. A notable and popular example

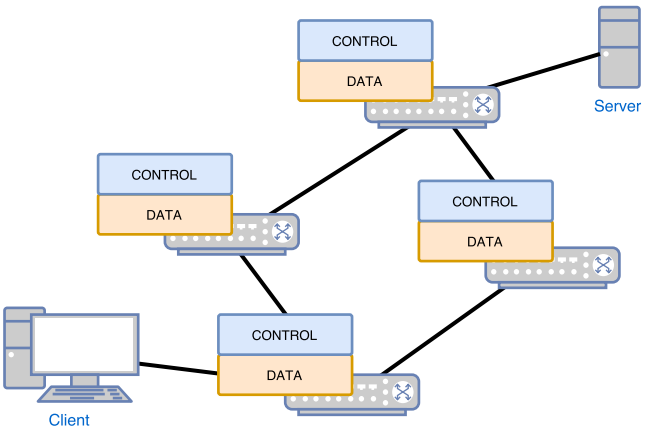

Figure 4: Conventional network architecture.

of such a kind of API is OpenFlow [132], an open-source solution which has been adopted for a large number of SDN-based prototype applications. OpenFlow supports the neat separation of control logic from the underlying physical devices. This change of perspective enables network designers and managers to write high-level software functions controlling the behavior of network infrastructures for industrial and cyber-physical systems and can be one of the main innovation for future CPS communications in order to:

- provide flexibility for communications and maintenance of communication activities, as requested for IIoT;
- allow for easier and dynamic reconfiguration of factories and plants, as needed for smart manufacturing and highly customized products.

Besides improving compatibility, reducing forwarding delays and hardware costs, SDN can impact significantly on telecommunication companies by changing current business models and generating new opportunities. Moreover, at present SDN appears to be the only solution which is really able to support systems where machine-to-machine communications are organized in such a way that resembles social networks as foretoken by many papers about IIoT [133], [134].

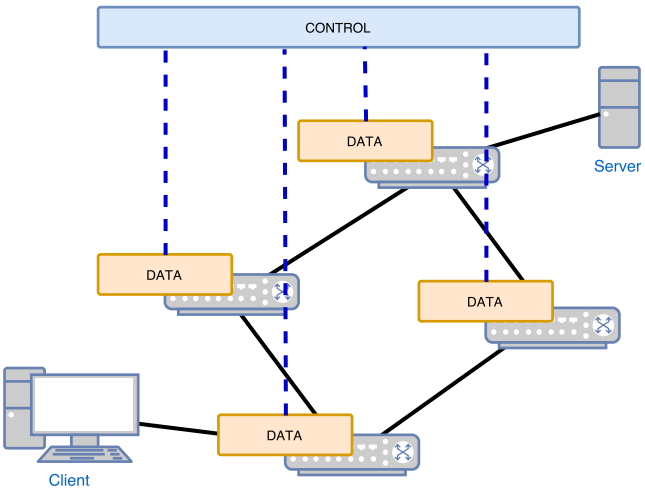

Figure 5: SDN-based network architecture.

SDN is also attracting significant attention from both academia and industry. For instance, a group of network operators, service providers and vendors have recently created the Open Network Foundation [135], an industry-driven organization aimed at promoting SDN and standardizing the OpenFlow protocol. Among the academic initiatives, instead, the Open Networking Research Center [136] has been created to focus on SDN research.

The reader interested in SDN can refer to [7] and [137] for comprehensive surveys which, starting from context and motivations, introduces the main SDN concepts and differences from traditional networking solutions. Instead, a detailed description of the SDN paradigm and architecture, besides a historic perspective, can be found in [138].

Software-defined networking is not employed in real industrial applications yet, however some experimental prototypes have started to be developed and tested. For instance, reliability for real-time communication services has been tackled in [100], [101] and [103], where an SDN-based approach is presented, which is aimed at the implementation of a QoS framework in industrial networks. In particular, in those papers the authors propose a technique to separate routing and resource allocation and achieve hard real-time performance.

Their interesting solution makes use of a "queue link" network topology for representing the underlying physical link structure besides resource and QoS parameters. Available link resources (e.g., data rate and buffer memory) and QoS parameters (e.g., delay constraints) are assigned to a set of link QoS queues. A routing algorithm is then used to find the best paths satisfying hard real-time requirements. The model was validated through simulation and network calculus [129], and compared to a more traditional approach based on mixed-integer programming (MIP).

Another approach oriented to achieve enhanced reliability through the SDN paradigm, leveraging standard hardware components in an experimental setup, has been described in [102], where a modified MAC is proposed. The authors' solution relies on traditional TDMA enhanced by the SDN availability of topology information and standardized SDN interface, that enable the installation of customized and application-specific routes in the network. Multiple devices are also allowed to send data simultaneously over physically separated links, thus introducing a Space Division Multiple Access (SDMA) element in the network architecture. In this way, hard RT communication is guaranteed by the TDMA scheme, while SDMA ensures an optimal use of the network and the whole architecture can be scaled efficiently. Obviously, all that glitters is not gold. The central controller introduces scalability issues that may be solved with physically-distributed control plane architectures, but, in doing so, consistency problems between different controllers may arise. Some solutions were proposed whose descriptions can be found in [139] and in [140]. These papers analyze the state-of-the-art of techniques to minimize the control to data planes communication overhead and controllers' consistency traffic so as to enhance the OpenFlow-SDN scalability.

Network Function Virtualization (NFV) is another concept which is often met jointly to SDN. The main underlying idea is to make virtual also those network services traditionally runnning on proprietary, dedicated hardware. As NFV affects the implementation of network functions, by removing the need of special-purpose hardware, network managers can add, move and/or change

them at the server level in a simplified provisioning process. Advantages of NFV were originally presented by a group of network service providers at the SDN and OpenFlow World Congress in October 2012.
The survey in [141] focuses on NFV and, in particular, deals with the definition of a reference architecture, introducing some use cases and a management and orchestration (MANO) framework.

6.3. Network of Networks (NoN), Cloud and Fog Computing

Basically, the underlying communication architecture in IIoT is conceived as a network of networks (NoN) with connections between subsystems (inter- and intra-enterprise) and of industrial devices (e.g., controllers, sensors, actuators) inside the same subsystem (i.e., shopfloor, control layer etc) [3]. As such, it has to be designed so as to enable extensibility of services and scalability. A preliminary attempt in this direction is presented in [142], where a combined approach between autonomous control and IoT for a logistic network is discussed. In factory automation this means new attractive opportunities to better coordinate and optimize operations for more efficient and cost-effective production [105]. A basic idea of IIoT is the ubiquitous accessibility of every type of information (e.g. sensor are made directly accessible to the ERP layer if needed). This means that information flows continuously from sensors to servers and processing units, while functional parameters are constantly updated thus reminding a comprehensive closed-loop system. From this point of view, approaches aimed at combining IIoT with emerging technologies, such as SDN, have started to appear. For instance, in [40] these aspects have been analyzed taking into account the network size and application complexity.

The network of networks will also allow the analysis and processing of data, collected from a universe of sources, to better understand dynamically changing requirements and drive the overall production in a fully automatic way by means of machine learning and data mining techniques [143]. From the scientific point of view the challenging NoN area is where the network self-awareness, self-management and self-adaptation issues mentioned in Sect. 4 have to find

satisfactory solutions and needs massive attention by the research community.

Cloud computing [144] and fog computing [145] are two other emerging concepts affecting IoT, in general, and IIoT in particular. The cloud can be thought of as a network of remote servers hosted in the Internet and used to store, manage, and process data in place of local servers or personal computers. The fog concept is similar to the cloud but reminds a phenomenon closer to the ground. The idea, in this case, is to have services closer to the data sources, but able to manage data at a network level through smart devices and on the end-user client side (e.g. mobile devices), instead of sending data to a remote location for processing.

New models necessarily mean new problems to be solved. As an example, authors in [106] present a cloud based-scheduling strategy for the Industrial Internet of Things. In particular, they model the task scheduling as an energy consumption optimization problem, taking into account task dependency, data transmission, response time, deadline and cost. A performance evaluation carried out using simulations shows how this solution is better than a baseline approach. Authors in [107] discuss emerging challenges in data processing, secure data storage, efficient data retrieval and dynamic data collection in IIoT. Then, they propose a framework to integrate fog and cloud computing. Their approach is based on processing data with either edge or cloud servers depending on their latency requirements, with a pre-processing phase of raw data. In particular, time-sensitive data (e.g., control information) are stored and used locally, while other data are transmitted to cloud servers for subsequent retrieval and mining activities.

The battery capacity of nodes is a research topic of interest for fog computing, for instance when the network is configured. In [108] authors present some strategies to overcome energy issues arising in battery-powered fog nodes. They propose an algorithm, based on both Lyapunov optimization function and parallel Gibbs sampler, to optimize service hosting and task admission decisions.

6.4. Peculiarities in Industrial Cybersecurity

Cybersecurity has been receiving considerable attention by researchers and professionals since several years and cannot be considered something new to several extents. In perspective, however, innovative approaches are needed in order to cope with IIoT and Industry 4.0. Till now, in fact, many investigation activities have focused on methodologies, techniques and mechanisms to analyze and mitigate risks, to design and implement security policies, to protect systems and devices and/or to develop effective countermeasures to attacks. In next generation networks, security strategies have to shift to a more global level, which is able to take into account a whole complex NoN consisting of several heterogeneous interacting subsystems with different administration domains and under the responsibility of different authorities.

Industrial systems security encompasses aspects as diverse as the protection of physical infrastructures and processes, communications protocols, asset management, or software and hardware lifecycle management, which cannot be handled in the same way as in their conventional IT counterparts. The peculiarities of industrial networks prevent the adoption of classical approaches to their security and, in particular, of those popular solutions that are mainly based on a detect and patch philosophy. For example, since availability is a top priority in ICSs as costs can increase dramatically in the case production is slowed down or even stopped, typical routine updates and/or hardware/software patching are frequently ignored in many plants and factories.

A comprehensive assessment of security in industrial networked systems was presented in [9] and the interested reader can refer to that paper for details. From a practical point of view, security key concepts such as availability, integrity and confidentiality (which are well-known in office and business networks) have to be considered with different priority levels. [9] also shows that cybersecurity is a cyclic process that has to be constantly applied to assure a satisfactory protection level for industrial systems in the years to come. Of course, security costs have also to be taken into account: [146] proposes some cost evaluation techniques and applies them to a case study of a real company

that sells products all over the world.

As awareness about the need for industrial cyber-protection is constantly rising, more and more papers can be found in the literature that deal with countermeasures to detect menaces and respond to attacks. For instance, a detection system based on the automatic deployment of honeypots is described in [110], which is able to examine the control system network in a passive way. The authors' solution is based on Honeyd [111], a small software daemon able to act as a virtual server with basic functionality. The Honeyd version developed in [110] is self-configured automatically to emulate any user-defined host in the network under analysis. The resulting architecture was also tested and evaluated on a small smart grid consisting of several types of devices (e.g., MS-windows-based PC, Rockwell and National Instruments PLCs).

Cybersecurity is already a major concern for SCADA and ICS managers, as the number of successful attacks against industrial targets is constantly growing. Currently, most popular and widespread SCADA protocols adopted for communications between industrial devices are insecure by design. For example Modbus [147], which is widely used at the application level in factories and plants because of its simplicity, is inherently insecure. Excluding the possibility of a complete replacement of these protocols, in the next years at least, and also considering the expected smooth migration of current factories to the smart scenario, an attempt to overcome this problem was presented in [109] where a security framework was developed, which is based on a distributed intrusion detection system. In particular, the proposed architecture consists of a first detection level (with domain-specific honeypots and specialized monitoring devices) and a second layer able to analyze events received from detection agents. The second layer makes use of machine learning techniques based on a one-class support vector machine (OCSVM) [112], and leverages topology and system-specific detection mechanisms which also consider the role, placement and behavior of the control system components.

Another kind of approach to SCADA security was presented in [113], which relies on a cybersecurity modeling language (CySeMoL) analysis tool. A prob-

abilistic relational model (PRM) is adopted to support operators of a security system in risk analysis. Starting from the architectural model, the tool can estimate the probability of successful attacks to the system according to different approaches. One appealing characteristic is that the model can be created without any specific security expertise. The system is then able to evaluate several kinds of attacks to ICSs including software exploits, flooding attacks, acquisition of wrong privileges and social engineering attacks. CySeMoL was experimentally verified and validated, and a better predictive version of the tool was also developed and described in [114].

The idea of introducing cybersecurity as a fundamental requirement already at the very beginning of any industrial system conception is progressively gaining consensus. This implies a radical change in the way of thinking, since at present security is mainly dealt with as a sort of add-on. Research and effort have to focus on techniques and tools for the analysis and management of security at a global system level. One important topic, from this point of view, is access control, since managing "who is allowed to do what on what" is the core of any protection scheme. In this context, the verification of policy correct implementation is a critical issue to determine whether users are actually forced to interact with the system in strict accordance with the access policies. This kind of security analysis, given the size and complexity of future systems, cannot be carried out by hand. In [115] a new methodology was presented for the semi-automatic verification of access control policies in industrial networked systems. The approach is based on a model which combines two different views (high and low levels) of the considered industrial system. In particular, policies are specified according to the standardized role-based access control (RBAC) framework [148], while the target system is described in tiny details through its low-level mechanisms. An automated software tool, purposely developed, helps the designer in performing the verification and finding fixes to errors and inconsistencies. The proposed framework was also evaluated in terms of complexity and performance to show its applicability to real-world industrial systems.

Defense techniques currently adopted in industrial systems are based on net-

work segmentation and partitioning to create demilitarized zones (DMZs), at different hierarchical levels. Firewalls (FWs) are main hardware and/or software components used to this purpose. However, the introduction of firewalls in industrial networks can cause unwanted side-effects, even when devices are employed that were explicitly designed for industrial environments. As more and more FWs are going to be deployed in future factory networks careful investigations should be carried out about their expected and actual behavior. In last years, some devices (industrial FWs) have been put on the market, that are able to recognize and analyze typical application protocols used in industrial environments. However, their inspection capabilities have to be evaluated in conjunction with the impact they have on the overall network performance. This aspect has been investigated in [116], where a simple technique based on COTS equipment and open source software has been developed to get useful information about effects produced by the introduction of a commercial industrial FW into an existing system. The proposed approach can be used in predicting operating margins and performance, moreover it can also be applied to analyze other devices available on the market.

6.5. 5G Networks and Slicing

Unconstrained mobility can be achieved only through the adoption of wireless technologies and, likely, by leveraging the new promising fifth generation mobile communication architectures. 5G [88] is expected to become a star performer for Industry 4.0 [61], in particular to enable ubiquitous communication and turn manufacturing processes into a sort of global distributed systems, characterized by strong interconnection, low-energy components and highly integrated logistics. Researches about 5G are being carried out to offer solutions for implementing integrated smart environments interconnecting smart factories, smart grids, smart buildings and logistics systems. The ability to cover wide areas should wipe out distances making, for instance, M2M communications integrated in the whole production chain. To achieve these goals, however, underlying communication infrastructures have to grant low latency, high band-

width and resilience.

Current technologies used in industrial environments are not sufficiently integrated to provide adequate support for all these aspects. In perspective, most appealing solutions seem those based on combined techniques able to leverage both wireless and wired communication systems, through public and private 5G providers. It is worth reminding that 5G is much more than mobile Internet: in fact, 5G networks integrate different communication media (e.g., mobile, wired, satellite), frequency bands and capabilities.

A preliminary analysis about the adoption of 5G and its impact on latency in IIoT and factory automation can be found in [90]. Instead, [91] deals with the combination of SDN and 5G networks to enable resource coordination across multiple domains, a key factor for Industry 4.0 applications too. A combination of 5G with fiber optic networks (fiber-wireless - FiWi) looks promising to enhance scalability, reliability, and energy efficiency at the same time [89], [93].

Possible use cases concerning industrial automation, control systems and M2M communications are described in [92]. These examples take advantage of the 5G capabilities for three different types of integration [149], namely: horizontal (e.g., connectivity to support inter-industry and supply chains, from raw materials to finished products ready for customers), vertical (e.g., linking of multiple production systems within the same manufacturer's boundaries, with customized user requests matched directly by new services in the manufacturer infrastructure) and end-to-end (e.g., full lifecycle process where both product and business service are conceived, designed, built, delivered and disposed) [150]. To be fair, 5G technologies look far from being adopted in industrial applications, as relatively few examples exist of their migration from theory [97] to experimental platforms [96]. Nevertheless they should be considered as one of the most disruptive contribution to wireless communication in the years to come.

The network slicing paradigm is often referred to as 5G networks. Roughly speaking, network slicing can be thought of as several virtual networks which share the same physical infrastructure for access and transportation. In prac-

tice, this is the introduction of the SDN concepts in 5G architecture, so that each type of application can be assigned an optimal network configuration for managing the related traffic. Network slicing also implies the coexistence of dedicated as well as shared "slices" in the network. An in-depth analysis of the advantages and the impact of the slicing techniques on 5G network design is presented in [94], while a real 5G trial testbed based on the slicing paradigm in the Hamburg port area is described in [95].

7. Conclusions and open issues

Industrial communication technologies have always been progressing since several years, either to better satisfy changing needs in typical application scenarios, such as factory automation and distributed process control systems, or simply to cope with continuous requests for increased performance. Main goals of the fourth industrial revolution and IIoT clearly show that this evolutionary process must be sped up and extended to embrace new scientific areas and challenging technical topics, as neither new demanding communication requirements can be satisfied nor innovative applications can be enabled, by relying only on the support offered by communication technologies in use today.

Indeed the Industry 4.0 scenario requires satisfactory answers to a number of scientific issues that in part have been investigated since several years, while others have started to be considered only recently. The first group includes well-known aspects, methodologies and techniques for enhancing main network characteristics such as bandwidth, real-time behavior, flexibility, dynamic reconfiguration, security, safety and fault-tolerance. These topics, though belonging to the tradition of the research community, will receive renewed and increasing attention to overcome the limitations of current solutions that make them scarcely suitable for Industry 4.0 [151].

The second group, instead, involves aspects that are either relatively new or have not been studied extensively till now. In particular, they concern the "smart" side of Industry 4.0, which relies on the availability of smart networks with self-

awareness, self-management and self-healing capabilities. These include main issues such as real-time/time-critical wireless communications, 5G mobile networks, very low power-consumption and industrial cybersecurity.

At present, a number of solutions, that are deemed able to satisfy future needs, are being investigated and constantly enhanced, but important breakthroughs are needed and innovative technologies have to be developed for use in real systems.

Among the others, SDN seems to be able to change the network architecture perspective from a traditional monolithic approach, which is rigid, hard to manage and often vendor-specific, to a more flexible and open approach. Significant benefits are then expected from its adoption in factory environments, in terms of scalability, performance, robustness and security [137].

The demand for real-time support is another key challenge to be faced. In this case, Time Sensitive Networking appears to be an interesting approach to follow in order to develop adequate solutions. Actually, TSN has the potentiality to support both real-time and conventional traffic. TSN systems are able to offer different essential services and satisfy real-time demanding applications (e.g., motion control) and high bandwidth data exchanges (e.g., data produced by the IIoT multitude of sensors) at the same time and in the same network.

Finally, cybersecurity is a common denominator in the global and open scenarios to come, and new surveillance and defense techniques must be studied that are able to to grant protection against faults and malicious behavior at the system level [152].

8. References

[1] R. Neugebauer, S. Hippmann, M. Leis, and M. Landherr, "Industrie 4.0 - from the perspective of applied research," *Procedia {CIRP}*, vol. 57, pp. 2 – 7, 2016, factories of the Future in the digital environment - Proceedings of the 49th {CIRP} Conference on Manufacturing Systems.

[Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212827116311556

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey ," *Computer Networks* , vol. 54, no. 15, pp. 2787 – 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[3] C. Perera, C. H. Liu, and S. Jayawardena, "The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 4, pp. 585–598, Dec 2015.

[4] J. Sargent and A. Ahmed, "What Is IT for Social Impact?: A Review of Literature and Practices," *IEEE Technology and Society Magazine*, vol. 36, no. 4, pp. 62–72, Dec 2017.

[5] S. Kang and K. Kim, "Motion Recognition System for Worker Safety in Manufacturing Work Cell," in *2018 18th International Conference on Control, Automation and Systems (ICCAS)*, Oct 2018, pp. 1774–1776.

[6] P. Gaj, J. Jasperneite, and M. Felser, "Computer Communication Within Industrial Distributed Environment – a Survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 182–189, Feb 2013.

[7] D. Kreutz, F. M. V. Ramos, P. E. Verssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan 2015.

[8] R. Mijumbi, J. Serrat, J. Gorricho, S. Latre, M. Charalambides, and D. Lopez, "Management and orchestration challenges in network functions virtualization," *IEEE Communications Magazine*, vol. 54, no. 1, pp. 98–105, January 2016.

[9] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, Feb 2013.

[10] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A Survey of Recent Results in Networked Control Systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, Jan 2007.

[11] T. Sauter, "The Three Generations of Field-Level NetworksEvolution and Compatibility Issues," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3585–3595, Nov 2010.

[12] B. Galloway and G. P. Hancke, "Introduction to Industrial Control Networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 860–880, Second 2013.

[13] A. Willig, "Recent and Emerging Topics in Wireless Industrial Communications: A Selection," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 2, pp. 102–124, May 2008.

[14] A. A. Kumar S., K. Ovsthus, and L. M. Kristensen., "An Industrial Perspective on Wireless Sensor Networks A Survey of Requirements, Protocols, and Challenges," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1391–1412, Third 2014.

[15] S. Chen, R. Ma, H. Chen, H. Zhang, W. Meng, and J. Liu, "Machine-to-Machine Communications in Ultra-Dense NetworksA Survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1478–1503, thirdquarter 2017.

[16] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," *IEEE Access*, vol. 6, pp. 78 238–78 259, 2018.

[17] J. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: A Survey on the Enabling Technologies, Applications, and Chal-

lenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1504–1526, thirdquarter 2017.

[18] M. Felser and T. Sauter, "The fieldbus war: history or short break between battles?" in *4th IEEE International Workshop on Factory Communication Systems*, 2002, pp. 73–80.

[19] M. Felser, "Real-Time Ethernet - Industry Prospective," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1118–1129, June 2005.

[20] *Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3 - Communication Profile Family 3 (PROFIBUS & PROFINET)*, Jul. 2014, IEC 61784-2:2014.

[21] *Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3 - Communication Profile Family 13 (Ethernet POWERLINK)* , Jul. 2014, IEC 61784-2:2014.

[22] *Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3 - Communication Profile Family 12 (EtherCAT®)* , Jul. 2014, IEC 61784-2:2014.

[23] R. Zurawski, Ed., *Industrial Communication Technology Handbook (Industrial Information Technology)*, 2nd ed. CRC Press, 2014.

[24] *IEEE 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*, IEEE Computer Society Std., Dec 2016.

[25] "Bluetooth Core Specification v5.0," Bluetooth Special Interest Group, 2016. [Online]. Available: https://www.bluetooth.com/specifications/adopted-specifications

[26] S. M. Darroudi and C. Gomez, "Modeling the Connectivity of Data-Channel-Based Bluetooth Low Energy Mesh Networks," *IEEE Communications Letters*, vol. 22, no. 10, pp. 2124–2127, Oct 2018.

[27] L. Leonardi, G. Patti, and L. Lo Bello, "Multi-Hop Real-Time Communications Over Bluetooth Low Energy Industrial Wireless Mesh Networks," *IEEE Access*, vol. 6, pp. 26 505–26 519, 2018.

[28] "Industrial networks - Wireless communication network and communication profiles - WirelessHART^{TM}," International Electrotechnical Commission (IEC) 62591, 2016. [Online]. Available: https://webstore.iec.ch/publication/24433

[29] "Industrial networks - Wireless communication network and communication profiles - ISA 100.11a," International Electrotechnical Commission (IEC) 62734, 2014. [Online]. Available: https://webstore.iec.ch/publication/7409

[30] "Industrial communication networks - Fieldbus specifications - WIA-PA communication network and communication profile," International Electrotechnical Commission (IEC) 62601, 2011. [Online]. Available: https://webstore.iec.ch/publication/7243

[31] S. Petersen and S. Carlsen, "Wireless Instrumentation in the Oil & Gas Industry - From Monitoring to Control and Safety Applications," in *SPE Intelligent Energy International*, 2012.

[32] ——, "WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor," *IEEE Industrial Electronics Magazine*, vol. 5, no. 4, pp. 23–34, Dec 2011.

[33] J. Neander, M. Nolin, M. Bjorkman, S. Svensson, and T. Lennvall, "Wireless Vibration Monitoring (WiVib) - An industrial case study," in *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)*, Sept 2007, pp. 920–923.

[34] S. Carlsen, E. K. Jensen, A. Aardal, H. Yoshino, O.-H. Bjor, and H. Olsen, "Wireless Noise Surveillance - Development of Dynamic Noise Maps," in *SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility*, 2016.

[35] W. Ikram, N. Jansson, T. Harvei, B. Fismen, J. Svare, N. Aakvaag, S. Petersen, and S. Carlsen, "Towards the development of a SIL compliant wireless hydrocarbon leakage detection system," in *2013 IEEE 18th Conference on Emerging Technologies Factory Automation (ETFA)*, Sept 2013, pp. 1–8.

[36] G. Cena, A. Valenzano, and S. Vitturi, "Hybrid wired/wireless networks for real-time communications," *IEEE Industrial Electronics Magazine*, vol. 2, no. 1, pp. 8–20, March 2008.

[37] L. Seno, S. Vitturi, and C. Zunino, "Analysis of Ethernet Powerlink Wireless Extensions Based on the IEEE 802.11 WLAN," *IEEE Transactions on Industrial Informatics*, vol. 5, no. 2, pp. 86–98, May 2009.

[38] J. von Hoyningen-Huene and H. Heeren and L. Underberg and S. Dietrich and P. Kroos and A. Wulf and O. Wetter and R. Kays, "Timing Evaluation of Cascaded Industrial Communication Networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5497–5504, Oct 2019.

[39] S. Wang, J. Ouyang, D. Li, and C. Liu, "An Integrated Industrial Ethernet Solution for the Implementation of Smart Factory," *IEEE Access*, vol. 5, pp. 25 455–25 462, 2017.

[40] J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, and A. V. Vasilakos, "Software-Defined Industrial Internet of Things in the Context of Industry 4.0," *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7373–7380, Oct 2016.

[41] W. Dai, V. Vyatkin, J. H. Christensen, and V. N. Dubinin, "Bridging Service-Oriented Architecture and IEC 61499 for Flexibility and Interop-

erability," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 771–781, June 2015.

[42] J. Wan, S. Tang, D. Li, S. Wang, C. Liu, H. Abbas, and A. V. Vasilakos, "A Manufacturing Big Data Solution for Active Preventive Maintenance," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 2039–2047, Aug. 2017.

[43] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security - A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec 2017.

[44] Christin, Delphine, Mogre, Parag S., and Hollick, Matthias, "Survey on Wireless Sensor Network Technologies for Industrial Automation: The Security and Quality of Service Perspectives," *Future Internet*, vol. 2, no. 2, pp. 96–125, 2010.

[45] K. J. Park, J. Kim, H. Lim, and Y. Eun, "Robust Path Diversity for Network Quality of Service in Cyber-Physical Systems," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2204–2215, Nov 2014.

[46] T. Kohler, F. Drr, and K. Rothermel, "Consistent Network Management for Software-Defined Networking Based Multicast," *IEEE Transactions on Network and Service Management*, vol. 13, no. 3, pp. 447–461, Sept 2016.

[47] L. Silva, P. Pedreiras, P. Fonseca, and L. Almeida, "On the adequacy of SDN and TSN for Industry 4.0," in *2019 IEEE 22nd International Symposium on Real-Time Distributed Computing (ISORC)*, May 2019, pp. 43–51.

[48] F. Chiti, R. Fantacci, M. Loreti, and R. Pugliese, "Context-aware wireless mobile autonomic computing and communications: research trends and emerging applications," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 86–92, April 2016.

[49] M. Peng, Y. Li, Z. Zhao, and C. Wang, "System architecture and key technologies for 5G heterogeneous cloud radio access networks," *IEEE Network*, vol. 29, no. 2, pp. 6–14, March 2015.

[50] E. J. Khatib, R. Barco, P. Munoz, I. D. L. Bandera, and I. Serrano, "Self-healing in mobile networks with big data," *IEEE Communications Magazine*, vol. 54, no. 1, pp. 114–120, January 2016.

[51] T. Bangemann, M. Riedl, M. Thron, and C. Diedrich, "Integration of Classical Components Into Industrial Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 947–959, May 2016.

[52] M. Elattar, V. Wendt, A. Neumann, and J. Jasperneite, "Potential of multipath communications to improve communications reliability for internet-based cyberphysical systems," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept 2016, pp. 1–8.

[53] M. Elattar, T. Cao, V. Wendt, J. Jaspemeite, and A. Trchtler, "Reliable multipath communication approach for internet-based cyber-physical systems," in *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, June 2017, pp. 1226–1233.

[54] P. Lindgren, J. Eriksson, M. Lindner, A. Lindner, D. Pereira, and L. M. Pinho, "End-to-End Response Time of IEC 61499 Distributed Applications Over Switched Ethernet," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 287–297, Feb 2017.

[55] N. Finn and P. Thubert, "Deterministic Networking Problem Statement. Draft IETF Problem Statement," Internet Engineering Task Force, 2017.

[56] K. McPherson, "Real-time-capable data communication via OPC UA," 2016.

[57] C. E. Salloum, M. Elshuber, O. Hftberger, H. Isakovic, and A. Wasicek, "The ACROSS MPSoC – A New Generation of Multi-core Processors

Designed for Safety-Critical Embedded Systems," in *2012 15th Euromicro Conference on Digital System Design*, Sep. 2012, pp. 105–113.

[58] M. S. Mollison, J. P. Erickson, J. H. Anderson, S. K. Baruah, and J. A. Scoredos, "Mixed-Criticality Real-Time Scheduling for Multicore Systems," in *2010 10th IEEE International Conference on Computer and Information Technology*, June 2010, pp. 1864–1871.

[59] S. Mittal, "A Survey of Techniques for Cache Partitioning in Multicore Processors," *ACM Comput. Surv.*, vol. 50, no. 2, pp. 27:1–27:39, May 2017.

[60] D. Dasari, V. Nelis, and B. Akesson, "A framework for memory contention analysis in multi-core platforms," *Real-Time Systems*, vol. 52, no. 3, pp. 272–322, 2016.

[61] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, March 2017.

[62] L. D. Ghein, *MPLS Fundamentals*. Cisco Press, 2006.

[63] M. Mahajan and M. Parashar, "Managing QoS for Multimedia Applications in the Differentiated Services Environment," *Journal of Network and Systems Management*, vol. 11, no. 4, pp. 469–498, 2003.

[64] H. Yin, H. Xie, T. Tsou, D. Lopez, P. Aranda, and R. Sidi, "SDNi: A Message Exchange Protocol for Software Defined Networks (SDNS) across Multiple Domains," Internet Draft, Internet Engineering Task Force, June 2012. [Online]. Available: http://tools.ietf.org/id/draft-yin-sdn-sdni-00.txt

[65] L. Silva, P. Gonalves, R. Marau, P. Pedreiras, and L. Almeida, "Extending OpenFlow with flexible time-triggered real-time communication services,"

in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sep. 2017, pp. 1–8.

[66] N. Finn, P. Thubert, B. Varga, and j. Farkas, "DetNet - Deterministic Networking Architecture," Internet draft, Internet Engineering Task Force, August 2016. [Online]. Available: https://tools.ietf.org/id/draft-finn-detnet-architecture-08.txt

[67] G. Cena, I. C. Bertolotti, T. Hu, and A. Valenzano, "Fixed-Length Payload Encoding for Low-Jitter Controller Area Network Communication," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 4, pp. 2155–2164, Nov 2013.

[68] ——, "A Mechanism to Prevent Stuff Bits in CAN for Achieving Jitterless Communication," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 83–93, Feb 2015.

[69] F. Tramarin and S. Vitturi, "Strategies and Services for Energy Efficiency in Real-Time Ethernet Networks," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 841–852, June 2015.

[70] A. V. Aho, J. E. Hopcroft, and J. Ullman, *Data Structures and Algorithms*, 1st ed. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1983.

[71] T. Givargis and F. Vahid, "Platune: a tuning framework for system-on-a-chip platforms," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 21, no. 11, pp. 1317–1327, Nov 2002.

[72] M. Palesi and T. Givargis, "Multi-objective design space exploration using genetic algorithms," in *Proceedings of the Tenth International Symposium on Hardware/Software Codesign. CODES 2002 (IEEE Cat. No.02TH8627)*, May 2002, pp. 67–72.

[73] G. Palermo, C. Silvano, and V. Zaccaria, "Multi-objective Design Space Exploration of Embedded Systems," *J. Embedded Comput.*, vol. 1, no. 3, pp. 305–316, Aug. 2005.

[74] I. Assayad, A. Girault, and H. Kalla, "Scheduling of real-time embedded systems under reliability and power constraints," in *2012 IEEE International Conference on Complex Systems (ICCS)*, Nov 2012, pp. 1–6.

[75] S. Han, X. Zhu, A. K. Mok, D. Chen, and M. Nixon, "Reliable and Real-Time Communication in Industrial Wireless Mesh Networks," in *2011 17th IEEE Real-Time and Embedded Technology and Applications Symposium*, April 2011, pp. 3–12.

[76] R. Costa and J. Lau and P. Portugal and F. Vasques and R. Moraes, "Handling real-time communication in infrastructured IEEE 802.11 wireless networks: The RT-WiFi approach," *Journal of Communications and Networks*, vol. 21, no. 3, pp. 319–334, June 2019.

[77] S. Girs, A. Willig, E. Uhlemann, and M. Bjrkman, "Scheduling for Source Relaying With Packet Aggregation in Industrial Wireless Networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1855–1864, Oct 2016.

[78] F. Tramarin, S. Vitturi, M. Luvisotto, and A. Zanella, "On the Use of IEEE 802.11n for Industrial Communications," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1877–1886, Oct 2016.

[79] G. Cena, S. Scanzio, and A. Valenzano, "Experimental Evaluation of Seamless Redundancy Applied to Industrial Wi-Fi Networks," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 856–865, April 2017.

[80] L. Seno, G. Cena, S. Scanzio, A. Valenzano, and C. Zunino, "Enhancing Communication Determinism in Wi-Fi Networks for Soft Real-Time

Industrial Applications," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 866–876, April 2017.

[81] W. Ikram, S. Petersen, P. Orten, and N. F. Thornhill, "Adaptive Multi-Channel Transmission Power Control for Industrial Wireless Instrumentation," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 978–990, May 2014.

[82] S. Kurt, H. U. Yildiz, M. Yigit, B. Tavli, and V. C. Gungor, "Packet Size Optimization in Wireless Sensor Networks for Smart Grid Applications," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 3, pp. 2392–2401, March 2017.

[83] J. Yan, M. Zhou, and Z. Ding, "Recent Advances in Energy-Efficient Routing Protocols for Wireless Sensor Networks: A Review," *IEEE Access*, vol. 4, pp. 5673–5686, 2016.

[84] K. S. Adu-Manu, N. Adam, C. Tapparello, H. Ayatollahi, and W. Heinzelman, "Energy-Harvesting Wireless Sensor Networks (EH-WSNs): A Review," *ACM Trans. Sen. Netw.*, vol. 14, no. 2, pp. 10:1–10:50, Apr. 2018. [Online]. Available: http://doi.acm.org/10.1145/3183338

[85] G. Verma and V. Sharma, "A survey on hardware design issues in RF energy harvesting for wireless sensor networks (WSN)," in *2016 5th International Conference on Wireless Networks and Embedded Systems (WECON)*, Oct 2016, pp. 1–9.

[86] A. M. Abdal-Kadhim and K. S. Leong, "Application of thermal energy harvesting from low-level heat sources in powering up WSN node," in *2017 2nd International Conference on Frontiers of Sensors Technologies (ICFST)*, April 2017, pp. 131–135.

[87] P. Ramezani and M. R. Pakravan, "Overview of MAC protocols for energy harvesting wireless sensor networks," in *2015 IEEE 26th Annual Interna-*

tional Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Aug 2015, pp. 2032–2037.

[88] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, February 2014.

[89] H. Beyranvand, M. Lvesque, M. Maier, J. A. Salehi, C. Verikoukis, and D. Tipper, "Toward 5G: FiWi Enhanced LTE-A HetNets With Reliable Low-Latency Fiber Backhaul Sharing and WiFi Offloading," *IEEE/ACM Transactions on Networking*, vol. 25, no. 2, pp. 690–707, April 2017.

[90] P. Schulz, M. Matthe, H. Klessig, M. Simsek, G. Fettweis, J. Ansari, S. A. Ashraf, B. Almeroth, J. Voigt, I. Riedel, A. Puschmann, A. Mitschele-Thiel, M. Muller, T. Elste, and M. Windisch, "Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 70–78, February 2017.

[91] A. Rostami, P. Ohlen, K. Wang, Z. Ghebretensae, B. Skubic, M. Santos, and A. Vidal, "Orchestration of RAN and Transport Networks for 5G: An SDN Approach," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 64–70, April 2017.

[92] C. Mannweiler, L. C. Schmelz, S. Lohmller, and B. Bauer, "Cross-domain 5G network management for seamless industrial communications," in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, April 2016, pp. 868–872.

[93] J. Liu, H. Guo, H. Nishiyama, H. Ujikawa, K. Suzuki, and N. Kato, "New Perspectives on Future Smart FiWi Networks: Scalability, Reliability, and Energy Efficiency," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1045–1072, Secondquarter 2016.

[94] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker, "Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72–79, May 2017.

[95] P. Rost, M. Breitbach, H. Roreger, B. Erman, C. Mannweiler, R. Miller, and I. Viering, "Customized Industrial Networks: Network Slicing Trial at Hamburg Seaport," *IEEE Wireless Communications*, vol. 25, no. 5, pp. 48–55, October 2018.

[96] P. Mekikis and K. Ramantas and A. Antonopoulos and E. Kartsakli and L. Sanabria-Russo and J. Serra and D. Pubill and C. Verikoukis, "NFV-Enabled Experimental Platform for 5G Tactile Internet Support in Industrial Environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1895–1903, March 2020.

[97] R. W. L. Coutinho and A. Boukerche, "Modeling and Analysis of a Shared Edge Caching System for Connected Cars and Industrial IoT-Based Applications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2003–2012, March 2020.

[98] M. H. Farzaneh and A. Knoll, "An ontology-based Plug-and-Play approach for in-vehicle Time-Sensitive Networking (TSN)," in *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Oct 2016, pp. 1–8.

[99] R. Obermaisser, R. I. Sadat, and F. Weber, "Active Diagnosis in Distributed Embedded Systems Based on the Time-Triggered Execution of Semantic Web Queries," in *2014 IEEE 17th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing*, June 2014, pp. 222–229.

[100] J. W. Guck and W. Kellerer, "Achieving end-to-end real-time Quality of

Service with Software Defined Networking," in *2014 IEEE 3rd International Conference on Cloud Networking (CloudNet)*, Oct 2014, pp. 70–76.

[101] J. W. Guck, M. Reisslein, and W. Kellerer, "Function Split Between Delay-Constrained Routing and Resource Allocation for Centrally Managed QoS in Industrial Networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2050–2061, Dec 2016.

[102] E. Schweissguth, P. Danielis, C. Niemann, and D. Timmermann, "Application-aware industrial ethernet based on an SDN-supported TDMA approach," in *2016 IEEE World Conference on Factory Communication Systems (WFCS)*, May 2016, pp. 1–8.

[103] J. W. Guck, A. Van Bemten, and W. Kellerer, "DetServ: Network Models for Real-Time QoS Provisioning in SDN-Based Industrial Environments," *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1003–1017, Dec 2017.

[104] L. Silva, P. Pedreiras, L. Almeida, and J. Ferreira, "Combining Spatial and temporal dynamic scheduling techniques on wireless vehicular communications," in *2016 IEEE World Conference on Factory Communication Systems (WFCS)*, May 2016, pp. 1–4.

[105] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, "Internet of Things and Edge Cloud Computing Roadmap for Manufacturing," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 66–73, July 2016.

[106] C. Tang, X. Wei, S. Xiao, W. Chen, W. Fang, W. Zhang, and M. Hao, "A Mobile Cloud Based Scheduling Strategy for Industrial Internet of Things," *IEEE Access*, vol. 6, pp. 7262–7275, 2018.

[107] J. Fu, Y. Liu, H. Chao, B. K. Bhargava, and Z. Zhang, "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4519–4528, Oct 2018.

[108] L. Chen, P. Zhou, L. Gao, and J. Xu, "Adaptive Fog Configuration for the Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4656–4664, Oct 2018.

[109] T. Cruz, L. Rosa, J. Proena, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, and P. Simes, "A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2236–2246, Dec 2016.

[110] T. Vollmer and M. Manic, "Cyber-Physical System Security With Deceptive Virtual Hosts for Industrial Control Networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1337–1347, May 2014.

[111] N. Provos and T. Holz, *Virtual honeypots: from botnet tracking to intrusion detection*. Pearson Education, 2007.

[112] W. Shang, P. Zeng, M. Wan, L. Li, and P. An, "Intrusion detection algorithm based on OCSVM in industrial control system," *Security and Communication Networks*, vol. 9, no. 10, pp. 1040–1049, 2016, sCN-15-0550.R1. [Online]. Available: http://dx.doi.org/10.1002/sec.1398

[113] T. Sommestad, M. Ekstedt, and H. Holm, "The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures," *IEEE Systems Journal*, vol. 7, no. 3, pp. 363–373, Sept 2013.

[114] H. Holm, K. Shahzad, M. Buschle, and M. Ekstedt, " P^2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 626–639, Nov 2015.

[115] M. Cheminod, L. Durante, L. Seno, and A. Valenzano, "Semiautomated Verification of Access Control Implementation in Industrial Networked Systems," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1388–1399, Dec 2015.

[116] M. Cheminod, L. Durante, A. Valenzano, and C. Zunino, "Performance impact of commercial industrial firewalls on networked control systems," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept 2016, pp. 1–8.

[117] L. Drkop, J. Jasperneite, and A. Fay, "An analysis of real-time ethernets with regard to their automatic configuration," in *2015 IEEE World Conference on Factory Communication Systems (WFCS)*, May 2015, pp. 1–8.

[118] P. Danielis, J. Skodzik, V. Altmann, E. B. Schweissguth, F. Golatowski, D. Timmermann, and J. Schacht, "Survey on real-time communication via ethernet in industrial automation environments," in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, Sept 2014, pp. 1–8.

[119] M. Luvisotto, Z. Pang, and D. Dzung, "Ultra High Performance Wireless Control for Critical Applications: Challenges and Directions," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1448–1459, June 2017.

[120] *Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3 - Communication Profile Family 16 (SERCOS)* , Jul. 2014, IEC 61784-2:2014.

[121] *Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3 - Communication Profile Family 2 (CIP^{TM})* , Jul. 2014, IEC 61784-2:2014.

[122] *AIRCRAFT DATA NETWORK PART 7 AVIONICS FULL-DUPLEX SWITCHED ETHERNET NETWORK*, ARINC Industry Activities, Jun. 2005, ARINC 664 P7.

[123] *Time-Triggered Ethernet*, Nov. 2016, SAE AS 6802.

[124] HMS Industrial Networks, "Market Share Report," 2017. [Online]. Available: https://www.hms-networks.com

[125] R. Enns, M. Bjorklund, and J. Schoenwaelder, "Network Configuration Protocol (NETCONF)," Internet draft, Internet Engineering Task Force, Jun. 2011. [Online]. Available: https://tools.ietf.org/rfc/rfc6241.txt

[126] *IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks – Amendment 26: Frame Preemption - IEEE Std 802.1Qbu-2016*, IEEE Computer Society Std., Aug 2016.

[127] *IEEE Draft Standard for Local and metropolitan area networks – Frame Replication and Elimination for Reliability - IEEE P802.1CB/D2.8*, IEEE Computer Society Std., 2017.

[128] *IEEE Approved Draft Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks Amendment: Per-Stream Filtering and Policing - 802.1Qci-2017*, IEEE Computer Society Std., 2017.

[129] J.-Y. Le Boudec and P. Thiran, *Network Calculus: A Theory of Deterministic Queuing Systems for the Internet*. Berlin, Heidelberg: Springer-Verlag, 2001.

[130] H. Bauer, J. L. Scharbarg, and C. Fraboul, "Applying and optimizing trajectory approach for performance evaluation of AFDX avionics network," in *2009 IEEE Conference on Emerging Technologies Factory Automation*, Sept 2009, pp. 1–8.

[131] M. Bjorklund, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)," Internet draft, Internet Engineering Task Force, Oct. 2010. [Online]. Available: https://tools.ietf.org/rfc/rfc6020.txt

[132] OpenFlow, 2017. [Online]. Available: https://www.opennetworking.org/sdn-resources/openflow

[133] J. I. R. Molano, J. M. C. Lovelle, C. E. Montenegro, J. J. R. Granados, and R. G. Crespo, "Metamodel for integration of internet of things, social networks, the cloud and industry 4.0," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 3, pp. 709–723, Jun 2018.

[134] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, Nov 2014.

[135] Open Networking Foundation, 2017. [Online]. Available: https://www.opennetworking.org/

[136] Open Networking Research Center, 2017. [Online]. Available: http://onrc.stanford.edu/

[137] J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark, G. Riley, and H. L. Owen, "Advancing Software-Defined Networks: A Survey," *IEEE Access*, vol. 5, pp. 25 487–25 526, 2017.

[138] B. A. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1617–1634, Third 2014.

[139] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN Control: Survey, Taxonomy, and Challenges," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 333–354, Firstquarter 2018.

[140] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, "Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey, year=2019," *IEEE Access*, vol. 7, pp. 107 346–107 379.

[141] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. D. Turck, and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 236–262, Firstquarter 2016.

[142] Uckelmann, Dieter, Isenberg, M.-A., Teucke, M., Halfar, H., and Scholz-Reiter, B., *Autonomous Control and the Internet of Things: Increasing Robustness, Scalability and Agility in Logistic Networks.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 163–181.

[143] I. H. Witten, E. Frank, M. A. Hall, and C. J. Pal, *Data Mining: Practical Machine Learning Tools and Techniques*, 4th ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2016.

[144] T. Hegazy and M. Hefeeda, "Industrial Automation as a Cloud Service," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 10, pp. 2750–2763, Oct 2015.

[145] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, Dec 2016.

[146] R. Leszczyna, "Approaching secure industrial control systems," *IET Information Security*, vol. 9, no. 1, pp. 81–89, 2015.

[147] Modbus Organization, "Modbus Protocol Specification V1.1b3," Available from http://www.modbus.org/specs.php, 2012.

[148] *Role Based Access Control - ANSI INCITS 359-2012*, ANSI, 2012.

[149] "White paper on 5G and the Factories of the Future," 5G-PPP, 2015. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Factories-of-the-Future-Vertical-Sector.pdf

[150] H. Kagermann, W. Wahlster, and J. Helbig, "Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0 – Securing the Future of German Manufacturing Industry," acatech – National Academy of Science and Engineering, Final Report of the Industrie 4.0 Working Group, 2013.

[151] V. K. L. Huang, D. Bruckner, C. J. Chen, P. Leito, G. Monte, T. I. Strasser, and K. F. Tsang, "Past, present and future trends in industrial electronics standardization," in *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Oct 2017, pp. 6171–6178.

[152] M. Cheminod, L. Durante, L. Seno, F. Valenza, A. Valenzano, and C. Zunino, "Leveraging SDN to improve security in industrial networks," in *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, May 2017, pp. 1–7.