IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 August 2022, accepted 13 September 2022, date of publication 3 October 2022, date of current version 19 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3211288

SURVEY

SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0

MLADEN ŠVERKO[1,2], TIHANA GALINAC GRBAC[3], (Member, IEEE), AND MILJENKO MIKUC[1], (Member, IEEE)

[1]Faculty of Electrical Engineering and Computing, University of Zagreb, 10000 Zagreb, Croatia
[2]Danieli-Systec d.o.o., Danieli & C. S.p.A., 52220 Labin, Croatia
[3]Department of Engineering, Juraj Dobrila University of Pula, 52100 Pula, Croatia

Corresponding author: Mladen Šverko (mladen.sverko@fer.hr)

This work was supported by the Croatian Science Foundation under Project HRZZ-IP-2019-04-4216.

ABSTRACT Recent technological advances encompassed by the smart factory concept have fundamentally changed industrial control systems in the way they are structured and how they operate. Majority of these changes affect Supervisory Control And Data Acquisition (SCADA) systems, shifting them to a higher level of interoperability, heterogeneous networks, big data and toward internet technologies and services in general. However, this transformation does not affect all SCADA systems equally. The immediate industrial environment and controlled processes have a significant impact as well. This paper presents a holistic approach to SCADA systems implemented in continuous flow production control within the steel industry production environment. We outline the multi-layer architecture of the SCADA control framework and the aspects of interoperability and interconnectivity within the architecture reference models, together with the research challenges and opportunities arising from the recent rapid increasement of the industrial control systems complexity and digital transformation under the Industry 4.0 paradigm, resulting in disrupting levels of the traditional automation pyramid based on Purdue model toward a higher level of integration and interoperability enabling cross-level data exchange empowered by the Industrial Internet of Things. Furthermore, the paper addresses the problem of proprietary SCADA systems and elaborates the causal correlation between SCADA quality requirements and adoption of new technologies in relation to the specific industrial environment of the steel manufacturing process.

INDEX TERMS Supervisory control and data acquisition, SCADA, supervisory control, data acquisition, industrial process control, cyber-physical, continuous flow production, manufacturing, steel industry, industry 4.0, industry 5.0, smart factory.

I. INTRODUCTION

In over three decades of their existence, Supervisory Control and Data Acquisition (SCADA) systems have undergone massive changes in their capabilities, structures, functionality and even in general perception and their role in the overall Industrial control system (ICS). Although this evolution has been gradual, the last decade has brought digital transformation in the field of industrial automation under the Industry 4.0 (I4.0) paradigm that has unleashed the full potential of SCADA systems within the smart factory concept based on the idea of merging the physical and virtual worlds interconnected and integrated across entire value chains leveraging on the new emerging technologies i.e. Internet of Things (IoT), Big data, Artificial intelligence (AI), cloud computing, service-oriented architecture (SoA) and cyber-physical

The associate editor coordinating the review of this manuscript and approving it for publication was Taous Meriem Laleg-Kirati.

systems (CPS) as core I4.0 enabling technologies [1]. All of these have been employed for the purpose of increasing the level of flexibility, autonomy, interoperability, equipment efficiency, product/process quality and overall productivity, i.e. to achieve an Intelligent management of the manufacturing process [2]

As a result of the smart factory concept implementation, Lean, Flexible, Sustainable, Digital, Cloud, Intelligent, Holonic, Additive and Agile manufacturing models have been defined [3], [4], based on utilization of specific groups of I4.0 enabling technologies and their impact on the entire industrial value chain.

While the I4.0 paradigm is still gaining momentum, further evolution leveraging on additional set of emerging enabling technologies [5] and enhancing solutions by combining current enabling technologies goes beyond technology-driven production efficiency, accomplishing merely economic goals, and extends to broader societal significance in an attempt to achieve resilient, sustainable and human-oriented concept of Industry 5.0 (I5.0) or Society 5.0 [6] in its wider context.

All of the above significantly impacts SCADA systems as well, leading to multiple concepts such as event-oriented, data-driven, model-driven, cloud-based, microservice-based and agent-based systems [7]. Each of these concepts are the result of different viewpoints and aspects such as quality requirements, available technology, process requirements, internal company policies, industry regulations, standardization and interoperability realities.

Furthermore, SCADA systems are built with intention to stand the test of time. The lifespan of the industrial automation system is expected to match the life of the industrial equipment. In that respect, SCADA systems are expected to go through multiple modifications, improvements and technological upgrades over time. The construction of such a flexible, robust and modular system requires comprehensive understanding of the system and solid grounds for SCADA system development in terms of applying architectural models based on generally accepted industry standards, and the use of equally standardized hardware and software components. The complexity of such a task is additionally emphasized by different domains of implementation, i.e. variety of industries that are significantly different in terms of quality requirements, production process, environmental conditions, industry standards, stakeholders, etc.

Under these circumstances, in terms of I4.0 reference architectures and approach to design and development of SCADA systems, it is not realistic to expect that a one-size-fits-all approach can produce satisfactory results across industries, regardless of how flexible a given model or concept might be. In this regard, based on research papers published in the Scopus and IEEE Xplore databases, industry-related websites, and the first author's two decades of experience in SCADA system development, this paper provides a comprehensive understanding of SCADA systems in continuous manufacturing process control with a focus on the steel industry domain and in the following aspects:

- Continuous flow production process and steel plant environment conditions related requirements for SCADA system in terms of architecture, integration, computational demands, accessibility, Industrial Internet of Things (IIoT), communication protocols and operators assistance.
- Impact of the I4.0 on SCADA architecture, network topology, communication protocols and standard automation pyramid i.e. ISA-95 (ISO 62264) model of functional hierarchies.
- Concept of the 4th generation SCADA systems in terms of the ISA-95 model transformation, integration of IIoT, CPS, cloud, services, and convergence of Information Technology (IT) and Operation Technology (OT) into heterogeneous networks.
- National initiatives and resulting international standards supporting reference architectural models within I4.0 and smart factory concept.
- The concept behind various reference architectures and mapping a standard SCADA system into Reference Architecture Model for Industry 4.0 (RAMI4.0) [8]
- SCADA-related concerns in manufacturing plant Industrial Control System (ICS) development life cycle.
- Conceptual understanding of I5.0 and the impact of human-centric approach to the next-generation SCADA systems.

Fig. 1 depicts the topics outline relative to the paper sections ending with key takeaways. Following the depicted content flow, the remainder of this paper is as follows. In Sect. II we provide basic understanding of the SCADA quality requirement related to the steel manufacturing process. Furthermore, we elaborate the horizontal integration, computational demands, accessibility, situational awareness, operator competence, IIoT and interconnectivity as requirements toward SCADA systems in control of the process in question. Sect. III continues with requirements resulting from the steel production facility's extreme environment conditions. Web SCADA, internet, cloud solutions and communication protocols are addressed.

Combined, these two sections aim to introduce industry domain-related conditions affecting SCADA systems, and considerations in design that address these conditions. Both of these are prerequisites for further content to be narrowed down to the domain of application in the steel industry continuous manufacturing process.

SCADA architecture is discussed in Sect. IV, beginning with technology-driven evolution over four generations of SCADA systems, followed by the integration of the I4.0 enabling technologies and thus transforming the traditional automaton pyramid. The I4.0 architectural reference models and their significance for SCADA systems in the steel industry domain are discussed in continuation, with topic extension to resulting ISO/IEC standards. As a predominant reference model, the RAMI4.0 is addressed in particular, with regard to the mapping of 3rd generation SCADA systems enhanced by the IIoT, cloud and services integration.

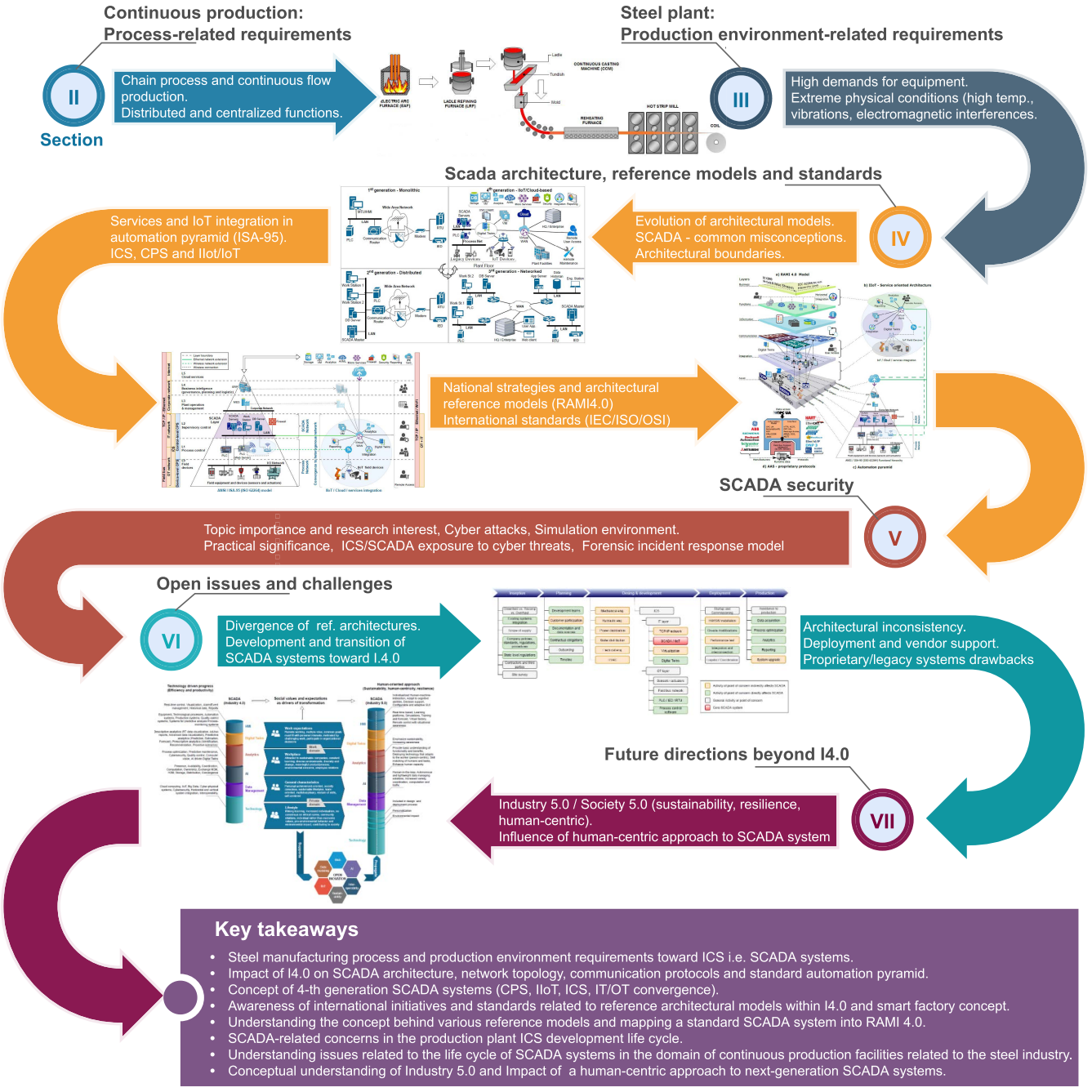


FIGURE 1. Topics outline relative to paper sections.

Sect. V addresses security in the domain of ICS/SCADA systems focusing on cybersecurity aspect and gives a brief information on research directions and their practical significance in domain of industrial environment, including implementation of the forensic incident response model. This topic, otherwise of great practical importance for today's industrial domain, has been reduced due to its extensiveness, which requires a comprehensive approach beyond the scope of this paper.

Open issues and challenges related to SCADA systems life cycle are considered in Sect. VI, with emphasis on development and deployment within the broader context of production facility ICS development, together with issues of proprietary and legacy systems drawbacks.

With regard to future trends, Sect. VII deals with key aspects of the Industry 5.0 paradigm and the broader significance encompassed by the Society 5.0 concept. Narrowing it down to the SCADA system, we explore the impact of social

values and expectations, i.e. the human-centric approach of I5.0 to SCADA system transition from I4.0 to I5.0 concept leveraging on emerging technologies.

The objective of such a structured context is to provide a comprehensive understanding of SCADA systems in an industry-specific domain of continuous manufacturing process control, and to address specific quality requirements for design of such SCADA systems taking into account the broader concepts of I4.0 architectures, enabling technologies and issues that are to be expected in SCADA system life cycle, emphasizing transition of previous generation SCADA system toward RAMI 4.0-compliant system which is significant for the majority of currently existing SCADA systems that are gradually advancing toward the Smart factory concept by enhancing the system with the partial integration of emerging technologies.

II. CONTINUOUS FLOW PRODUCTION PROCESS RELATED REQUIREMENTS

Leaving aside the technological progress, the Industry 4.0 (I4.0) paradigm and the smart factory concept, the industrial environment and the manufacturing process itself have a significant impact on the direction of future development, the architecture and the structure of the SCADA systems, the selection of newly available technologies and the way they are adopted and integrated to achieve the system requirements. To some extent, this affects both the hardware and software of the entire ICS. In the industrial environment of continuous manufacturing processes in the steel industry, the approach to the SCADA system design, development and deployment is significantly affected by: 1) The specifics of the continuous flow production process and 2) The extreme physical conditions under which the ICS operates.

The process of steel manufacturing is not only complex, but it also combines chained processes and continuous flow production where all production zones greatly influence each other. This makes it highly demanding in terms of real-time process control and maintaining continuous material flow through all the zones.

Fig. 2 shows a simplified layout of the steel manufacturing process that includes an electric arc furnace (EAF) to produce molten steel, a ladle refining furnace (LRF) to adjust the chemical composition of the molten steel, continuous casting machine (CCM) to shape the steel into an acceptable form for the next production phase e.g. thin slab, reheating furnace (RF) to increase the temperature and hot strip mill (HSM) to produce the final product in the form of a coil to be further used as input material in steel mills of various types (cold rolling / reversing / tandem mill, hot deep galvanizing line, annealing line, coating line, etc.).

A. OVERLAP OF DISTRIBUTED AND CENTRALIZED FUNCTIONS

Although the representation of the process shown in Fig. 2 is simplified, a unique demand for distributed and yet centralized and the synchronized control stands out. As presented process consists of five separated production areas (EAF, LRF, CCM, RF, HSM) that operates independently on dedicated machinery, and each is complex enough to be monitored/interfaced by a separated human machine interface (HMI), therefore it is necessary to develop distributed control functions, i.e. SCADA system for each production unit, which is the usual practice. However, given the high level of causal correlation between these production areas, it is crucial to maintain close watch on the overall process in order to maintain a continuous flow of material and to avoid time delays between production areas when possible. To achieve this, centralized monitoring of key production parameters must be implemented at the SCADA level, allowing for a timely response to the next process phase in the chain or within the continuous flow.

Given the above demands, the solution of the central database is logically imposed. However, even if this may seem to be a practical solution for historical logging e.g. via SQL database, a central runtime database that encompasses all process variables exchanging values generated on plant floor in real time could be overwhelming task for SCADA network and may affect system response in moments of vast amount of real-time data exchange, e.g. when a new steel type is entering in production and forces majority of production process parameters to be modified.

B. INTEGRATION OF MANUFACTURING SCADA SYSTEM AND SUBSTATION AUTOMATION SYSTEM

Another requirement imposed by the nature of the process is partial integration of manufacturing control systems with cyber physical systems (CPS) at the level of substation automation i.e. power monitoring systems (PMS) at plant level. Power consumption plays a big role in EAF and LRF part of the presented process, and directly affects the manufacturing process quality and performance. In the case of EAF, energy consumption can reach close to 500 kWh/t of steel [9] (EAF without oxyfuel burners) which gives a good motive for monitoring its value during production in real time. In addition, operators should have direct access to belonging feeders i.e. circuit breaker control accessible through the electrical substation automation system (SAS), or via centralized power control center (PCC) if such exists at the plant level.

Considering the differences between SCADA systems, network protocols and security issues in general industry automation vs. the energy sector, this is not an easy task with existing proprietary SCADA systems with limited interoperability between systems from different vendors, which is especially emphasized in the case of partial s of legacy control systems that act as an integrated part of the larger ICS.

C. COMPUTATIONAL DEMANDS AND ACCESSIBILITY

In addition to the overall layout of the process, Fig. 2 includes a detail of the mold, showing adjustable sides and real-time monitoring of the heat distribution (heat map) of the steel inside the mold. The purpose of this is to illustrate one of the computational demanding tasks taking place in the CCM

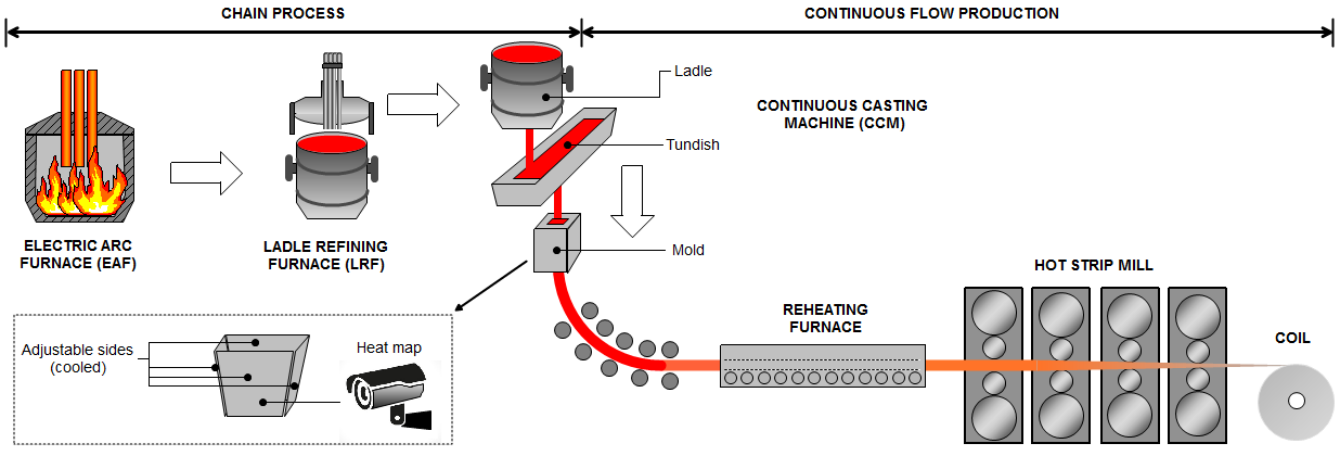


FIGURE 2. Steel manufacturing process.

area. The molten steel running through the mold that shapes it, presents one of the critical points in the controlled process due to the risk of steel sticking to the inner surface of the mold, and thus forming a ''cold tooth'' or breaking and causing ''Steel Leakage'' when the shell of the cast stream ruptures and causes one of the main operational failures. To prevent all of the above, this segment needs to be monitored and adjusted as the steel flows through the mold by mold cooling, steering, oscillation frequency and curve form. In order to achieve this, the control system needs to be fed with data from the temperature sensors network forming a heat map, i.e. indirect measurement of the steel condition inside the mold. Stability, reliability, availability and low response time are crucial requirements that the SCADA system must provide in this case.

Even though this example illustrates the production process-related demands towards the development of the SCADA system, the computational aspect is even more emphasized in EAF area where electrodes adjustment algorithms combines neural networks, fuzzy logic and Proportional Integral Derivative (PID) control to cope with problem of non-linearity and time-varying characteristics [10]. There is nothing new in using Artificial Intelligence (AI) and machine learning (ML) in process optimization, but in the case of real-time data extraction from manufacturing SCADA systems, they need to become more accessible and open in this regard. There is no lack of motivation in that segment, since it has been proven that intelligent algorithms in the EAF electrode control system itself have increased productivity up to 20%, reduced electrode consumption by 0.4–0.6 kg/t, and reduced electrical energy consumption by 18–20 kWh/t [11].

D. SITUATIONAL AWARENESS AND OPERATOR's COMPETENCE

Great deal of industrial processes generate vast amounts of data on which SCADA systems depend in order to achieve set goals in process control. The steel industry is no exception in this regard. In order to reach necessary situational awareness required to achieve the adequate level of control, most of this data has to be present on the HMI user interface.

In the field of continuous steel manufacturing process, this is particularly evident in strip processing lines such as annealing, coating, galvanizing, pickling and chemical treatment lines [12] where the complete production line needs to be visible as a whole. As a simple practical solution, the increase of the GUI area is imposed, i.e. enlarging screens and the development of the HMI with multi-screen systems. However this easily generates oversized and cluttered production line overviews and further opens the question of human cognitive limitations when it comes to interpretation of such a complex and detailed schematic of an ongoing process and with limited time for operator to react to unforeseen situations.

There are studies dealing with the problem of situational awareness and human cognitive limitations in other areas and from different angles. Golan, Cohen and Singer [13] propose a new concept of operator-workstation for I4.0 that monitors operator's condition and provides estimation of his/her cognitive capabilities in relation to the condition of the monitored process. Reguera-Bakhache et al. [14] introduces the concept of an adaptive interface that reconfigures (declutter) in real time according to the user's current focus in relation to the ongoing process. The Increasing level of complexity in process control and user overload is recognized in the field of aviation industry as well, where the implementation of AI at the HMI level is proposed as an additional operator's support tool [15].

In respect to these researches and proposed solutions, there is another specific condition to consider when addressing the domain of situational awareness and human limitations in steel manufacturing. The aforementioned strip processing lines can physically span across several hundred meters, and therefore cannot be monitored from a single control room. As processing lines are usually divided into entry, process and exit sections, so are the control pulpits. Taking into account a minimum of two operators per control pulpit, three shifts,

24h non-stop production and stand-by team, we arrive at a total number of at least 24 operators needed for control of such a processing line. With that number of operators, a certain workforce fluctuation and possible outflow is expected. In addition, current needs may require the temporary relocation of operators between process sections, and it is unrealistic to expect each operator to know all the process segments equally well.

Considering the aforementioned increasing level of complexity when it comes to SCADA systems and HMI GUI, the general problem of an unequal level of operator competence stands out. Under these circumstances, a comprehensive training plan is expected to progress and keep up with the level of SCADA complexity. However, according to the World Steel Association sustainability indicators [16], employee training hours have stagnated around 7 days per year for a decade (2011–2021). Given the amount of new technology and principles implemented in that period under the I4.0 paradigm, this cannot be sufficient to achieve adequate operator competence in operating continuously evolving process control and SCADA systems. Furthermore, it directly affects overall team functioning, performance and ability for knowledge sharing which is important in extreme environments [17]. Under the given circumstances, the development of methods for raising the level of situational awareness by the SCADA systems applied in the metal industry must, in addition to human limitations, take into account the operator's limited knowledge of the controlled process. This directs the evolution of such methods, not only towards improving the information model of the controlled process, but also towards support in decision-making based on case-level domain knowledge. Considering the diversity of individual production areas within the same facility, system modularity is imposed as an additional requirement in order to achieve desired level of SCADA system flexibility needed to adapt to CPS changes over time.

E. INDUSTRIAL IoT (IIoT) AND INTERCONNECTIVITY

There are numerous benefits in process optimization, cost reduction, enhancing product and control quality [18], [19], and overall functionality from IIoT implementation in the I4.0 manufacturing plants, leveraging multiple information sources of interconnected devices and their computational capabilities.

Observing the core process of steel manufacturing, IIoT devices can facilitate field measurements and real-time process monitoring, provide a higher level of data quality in relation to the controlled process and to equipment status, enable more direct inter-layer and cross-layer communication across traditional automation pyramid, and achieve a higher degree of interoperability.

More specifically, the following points of the steel manufacturing process represented in Fig. 2 and subsequent lines and/or mills can be measured by IIoT devices that can replace the standard legacy sensor equipment used in plant field:

- Slab (thin-slab, billet, bloom etc.) and preheating heater temperature that can be instantly compared to product type enabling faster detection of potential quality issues.
- Material flow from mold (and/or tundish) enabling greater efficiency in maintaining the continuity of the entire process from EAF and raw materials input, to the final product.
- Rolls gap measurement (between working rolls on each stand as shown in HSM) that can be instantly compared across the line (by direct communication between field devices) greatly influences the timely application of corrective measures.
- Sheet width, thickness, profile and deformation measurement along the strip line using IIoT devices in collaborative manner can significantly speed up detection of errors in the overall measurement system and prevent the continuation of the production of defective products.
- Coil radius, sagging of a steel sheet or similar position-related measurements by IIoT device may not give more accurate or better result in comparison to standard field sensors, but speed or torque control, crucial for maintaining continuity of the line operation is extremely time-critical and the ability to unify all key measured device under same communication platform greatly improves the chances for a timely reaction of automated control system.

The aforementioned use of IIoT devices is not a novelty within the concept of a smart factory, and although traditionally IIoT devices do not belong to the SCADA system, their communication and computing capabilities transcend the standard operation an information technology (OT/IT) division within ICS, and greatly influence communication protocols and cybersecurity [20], [21], [22], [23], [24], design patterns and architecture of the future SCADA systems [25], [26], [27], [28] and shift the entire ICS toward big data, internet and cloud solutions [29], [30].

From the steel manufacturing process point of view, it makes sense to make advantage of interlayer communication, i.e. direct communication between IIoT devices and their computational power, to feed the core SCADA processes with intermediate and structured calculation results generated on fog layer [31] rather than a large quantity of raw measured data that negatively influence network performance, i.e. reducing the network latency at the same time. An additional benefit comes from the IIoT devices metadata that play a significant role in building blocks for predictive maintenance frameworks [32].

III. STEEL PLANT ENVIRONMENT CONDITIONS RELATED REQUIREMENTS

The physical conditions inside the production facility can be seen as a consequence of the production process, which in the case of steel plants can be classified as extreme [33]. As such, the steel manufacturing process imposes high demands on plant equipment on the production floor [34],

but consequently also on network and SCADA systems, and therefore posing an industry-specific requirement that shapes the future development of various system control segments.

A. WEB SCADA, INTERNET AND CLOUD SOLUTIONS

The steel manufacturing process involves extremely high temperatures. The electric arc furnace [35] generates temperatures reaching 1800°C and up to 1700°C when the molten steel is transferred to the casting floor, i.e. tundish and mold. Major part of the SCADA equipment is not exposed to such extreme temperatures near EAF, but HMI control panels are standard equipment on casting floors. In addition to extreme temperatures, strong vibrations in the production process shown in Fig. 2 are generated at the casting floor caused by mold oscillating frequency of 0.5 Hz which significantly affects the surrounding equipment and posses a serious challenge for SCADA components i.e. controls panels that are usually mounted on movable arms and hanging in proximity of oscillating molds.

Under these conditions it is highly desirable for SCADA systems to use only minimal hardware and software configuration on casting floor, and benefit from remote access and virtualization solutions relying on redundant client-server architecture [36], and potentially moving toward cloud solutions [37], [38], [39] providing additional storage and computational power.

B. HARDWARE, IIoT AND COMMUNICATION PROTOCOLS

Another negative impact affecting IIoT devices and SCADA systems comes in the form of electromagnetic fields (EMF) i.e. electromagnetic interference (EMI) [40]. When it comes to the subject of EMI and IIoT, the spectral noise level, and consequently radio interference between IoT devices is the primary concern [41], along with electromagnetic compatibility [42].

However, in the case of steel plants there are additional sources of potential EMI such as the radioactive mold level detector, the mold steerer and molten steel itself. To a certain extent, steel presents an obstacle to the propagation of radio waves. This is rather normal in an industrial environment that has a metal construction of the facility and installed machinery, and this is taken into consideration when building industrial IoT systems for the factory floor. But in the case of a steel plant, these obstacles are dynamic and they move across the production facility. The ladle passes the distance between EAF and CCM by moving across the plant while hanging on a crane with over 100 t of molten steel inside. Additionally, produced billets, blooms, coils, etc. are moving across the plant floor constantly as well.

This may not affect a standard SCADA system and network using shielded network cables, but most of IIoT devices are equipped with wireless technology that makes them vulnerable to such interference, and it can have unpredicted consequences that could be difficult to diagnose when manifested randomly if affected by random movements of massive equipment and products.

In communication to IIoT devices on the plant floor, the SCADA system needs accurate, reliable and timely data to perform its task. If there is even partially corrupted data coming from field devices, it affects not only real-time process control, but also time series analysis applied in various algorithms used for equipment reliability analysis i.e. predictive maintenance [43], [44], process optimization, condition monitoring [45], quality control [46], [47] and similar. Finally, this results in inaccurate aggregated time series stored in data historian [48], i.e. long-term archive.

These environmental conditions emphasize the importance of an adequate implementation of IIoT communication protocols in similar extreme production conditions. When it comes to IoT wireless devices, low power stands out as one of the major concerns, and thus protocols like Long Range WAN (LoRaWAN), Low-Power Wide-Area (LPWA) or Constrained Application Protocol (CoAP) are developed. But for given conditions, messaging pattern, mechanism, quality level and End-to-End packet delays are of greater importance. It is not expected that a single IoT protocol can be sufficient across the entire IoT network. However, the use of multiple protocols further rises the question of coexistence [49]

Considering the IoT protocol specification and compared results [20], [50], [51], [52], [53] there is still room for improvement to meet the specific needs of the industrial environment.

For example, the Message Queuing Telemetry Transport (MQTT) protocol defined under ISO/IEC 20922:2016 standard is a good fit for IIoT devices in the production floor, i.e. their communication to SCADA system, given its characteristics [20], [52], [53]:

- It is based on Ethernet and Wi-Fi infrastructure.
- Quality of Service (QoS) field defines the guarantee of delivery between sender and receiver.
- It supports three QoS – Most once (0), At least once (1), Exactly once (2).
- It supports exchanging messages between multiple clients through a central broker.
- Clients can subscribe to various topics and receive their associated messages.
- It is message-oriented, event-based and asynchronous model

The above attributes show that the MQTT protocol can meet the needs when it comes to reading data from multiple clients. However, in case the command signal needs to be sent back from the HMI on the subscriber side, the asynchronous publish-subscribe mechanism does not make this task simple in terms of development. Since response to the command can take a long time, this can cause the problem for the operator who does not have the information of performed action [54]. From the HMI development point of view, it is questionable how to treat these cases and what is the amount of delay that can be tolerated prior to warning the operator.

Another approach to corrupted data coming from field devices is the development of ML algorithms detecting

and describing the patterns that lead to abrupt changes in the behavior of sensor signals in specific operating scenarios [45].

IV. SCADA ARCHITECTURE

In the field of system engineering Shenhar and Sauser [55] provide a broader definition of architecture as a blueprint providing a current and future description of a domain composed of interconnected components, performing activities and associated constraints. Similarly, in the domain of Smart manufacturing architecture reference models, Li et al. [56] defines architecture as a model of basic arrangement and connectivity of physical or conceptual objects or entities. Following these general definitions, the fundamental purpose of the architecture is to provide a comprehensive overview of overall design with logical and physical interrelationships, not only to describe the system from multiple perspectives, but also to provide a useful set of principles and rules to be used as guidelines for future development and modifications of the progressively advancing system.

When it comes to SCADA system architecture, this task is not that simple to achieve. Not only has the SCADA system undergone significant changes over time [57] and it still does on a large scale, including various mitigation scenarios [37], but it is also an integral part of a larger ICS in which it is integrated across multiple hierarchical layers and extends even beyond ICS boundaries by exchanging data with enterprise-level IT solutions supporting business model and various cloud-based services supporting smart factory concept.

Apart from expanding across levels that have traditionally been rigidly defined within their functional boundaries of ISA-95 automation pyramide, i.e. ANSI/ISA-95 Enterprise-Control System Integration standard [58], there is also an increased level of connectivity, interoperability and integration resulting in the overall convergence of the SCADA system which subsequently expands in the range of advanced technologies, devices and services that should also be taken into account.

A. TECHNOLOGY DRIVEN EVOLUTION OF ARCHITECTURE MODELS

Following technological advancement SCADA systems have undergone changes over the four generations shown in Fig. 3: 1) Monolithic closed system with standalone HMI that acts as a mainframe system and communicates directly to PLC and RTU with proprietary communication protocols and software; 2) Distributed system introducing communication servers, separate mainframe, LAN, redundancy and increased computational power. Most of the software and network protocols are proprietary but less expensive and the system is more flexible; 3) Networked SCADA has expanded the LAN boundaries utilizing internet technologies and reaching out to WAN using standard TCP/IP protocol. Off-the-shelf and open source solutions are implemented, data becomes more accessible, and proprietary systems more open, but consequently exposed to cyber threats as well; 4) The fourth generation SCADA systems emerged from the smart manufacturing target capabilities such as agility, quality, productivity and sustainability [59] and Smart Manufacturing Ecosystem (SME) [56] derived from the functional and equipment hierarchy and the physical asset equipment model from the ISO/IEC 62264 standard, as introduced by the National Institute of Standards and Technology (NIST), implementing digital transformation (DX) under the umbrella of Smart factory and I4.0 paradigm. The resulting ICS comprises a subsystem comprising CPS, IIoT smart devices, cloud solution and services, AI / ML, virtualization platforms and rapidly increasing amount of data – all under the common concept of IIoT/IoT, cloud and services-oriented SCADA system.

A prerequisite for the design and standardization of such a system architecture, according to the aforementioned definitions, is unambiguous understanding of the elementary units/entities and connections as well as the functions and boundaries of the system.

B. INITIAL CONSIDERATIONS AND COMMON MISCONCEPTIONS

Crossing the traditionally defined boundaries of the SCADA system and spanning across the ICS layers, as well as the conceptual and physical expansion of the fourth generation SCADA systems, resulted in multiple ambiguous definitions that sometimes proceeds from attempts to provide a definition of ICS or SCADA systems under the I4.0 concept referring to inadequate architectures of previous generation control systems. This issue must be addressed and resolved prior to discussing the SCADA structure under the I4.0 paradigm.

Traditionally, ICS has been organized in hierarchical levels according to the Purdue model since the first SCADA generation in the form of isolated monolithic architecture. Such a division is in accordance with the ISA-95 hierarchy of functions and gives a solid ground for the vertical integration of ICS network and subsystems divided indo Field, Supervisory and Network layers, or Operational technology, Information technology and Enterprise networks respectively [60]. Extending the model to the I4.0, these layers can be interpreted as areas of shop floor, IT, and Industry 4.0. [61]. Thus defined, the model provides an overview and understanding of device functions and hierarchical position within the narrow area of implementation.

However, the above hierarchical model, suitable for vertical integration and cross-layers data flow, does not provide enough flexibility nor dimensions to provide a comprehensive explanation of ICS and SCADA system within a smart factory concept shifting to a peer-to-peer model of collaboration i.e. horizontal integration. Therefore, several doubts and ambiguous interpretations arise that can be reduced to three groups: 1) Defining the conceptual and functional boundaries of SCADA systems, 2) Understanding the differences between ICT, CPS, IoT and IIoT, 3) the relationship between IIoT and SCADA systems.

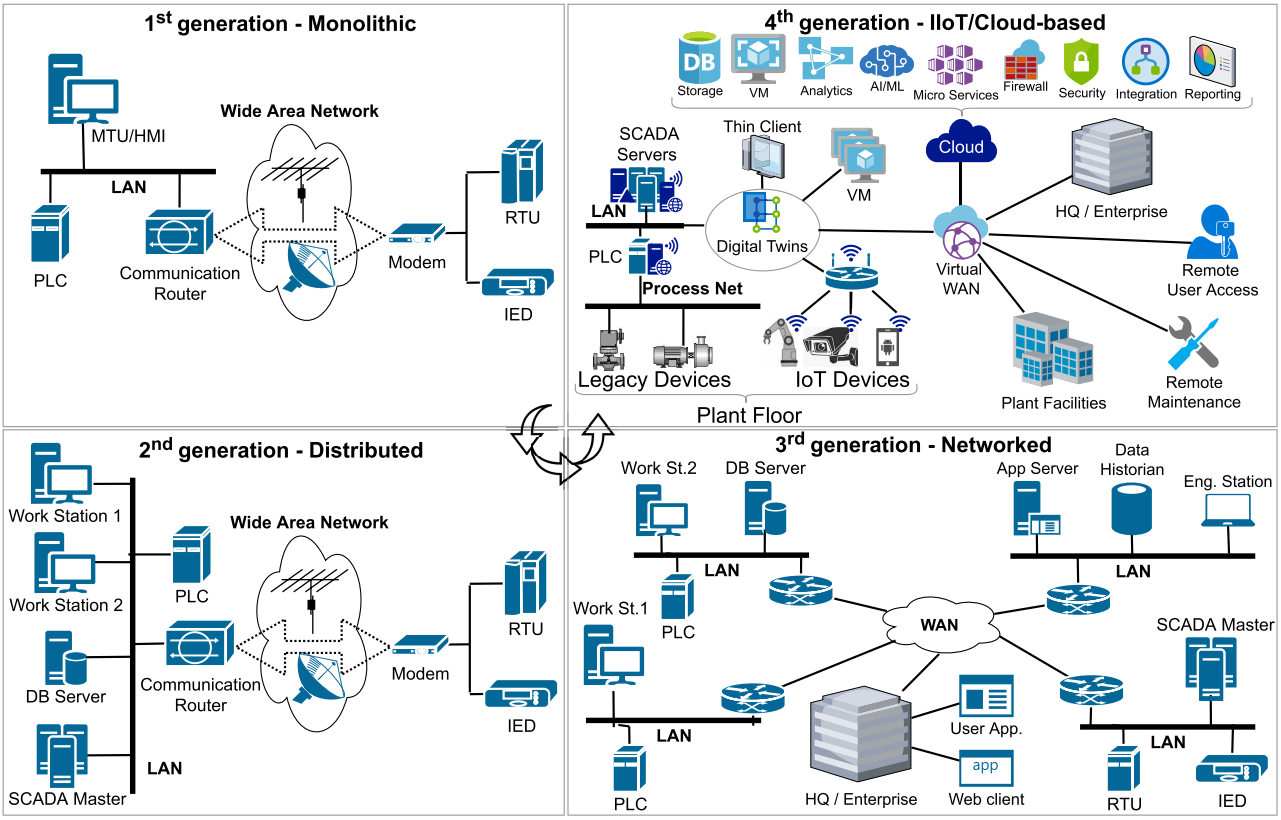


FIGURE 3. SCADA architectures.

1) SCADA SYSTEM ARCHITECTURAL BOUNDARIES

In an attempt to provide a structural and functional description of the ICS or SCADA systems, their domains and boundaries might be interpreted ambiguously. In some cases SCADA is equated with ICS [62], [63], or ICS is equated with OT which is also referred to as CPS [64], SCADA may be considered integrated with PLC or even extended downward to the RTU [65], [66], [67], [68]. In some cases, SCADA can also be considered a software component within the Simatic ecosystem [69].

These misconceptions are understandable due to overlapping functions. However this interpretation undermines the IT / OT division of ICS, which is crucial for process control QoS and understanding of SCADA system functionality. It is important to emphasize that OT refers to the control system that is in direct control of the industrial process i.e. manufacturing equipment on the plant floor, whereas IT extends process control to a higher level of the control system that includes the SCADA network and, together with OT, it forms ICS. In the traditional ISA-95 hierarchical model, the OT alone (with the addition of HMI) is capable of running the industrial process.

The IT/OT division clearly places SCADA away from the OT systems and therefore excludes PLCs and devices on the plant floor from the architecture design [60].

Although, under the I4.0 paradigm, IT and OT converge, this primarily refers to the implementation of IIoT technology and expansion of network capabilities, and does not change the key requirements of OT system that is mission critical and requires high-availability in relation to IT system to which the CIA-triad (confidentiality, integrity and availability) is becoming increasingly important due to exposure to cyber-threats. However, it does expand SCADA system boundaries by including IIoT devices on the plant floor into the SCADA network.

2) ICS, CPS AND IIoT/IoT

It is not uncommon for CPS to be equated to OT, or both to be considered equivalent to Industrial Automation and Control Systems (IACS) extending across the industries [64]. A similar understanding results in the concept of SCADA-driven CPS as a control system built on SCADA technologies [70], and refers to CPS as a "smart industrial system" that utilizes SCADA systems for control and monitoring [71]. Ali et al., in Cyber Security for Cyber Physical Systems [72], envisage conceptual illustration of ICS/SCADA infrastructure, and defines CPS as *"...a various collection of information communication technology (ICT) and embedded microprocessors which are communicated to the physical world via sensors and actuators"*. Thus defined, they consider CPS to be controlled by ICS/SCADA Systems. The above perceptions of CPS and ICS/SCADA integration are further emphasized by the inclusion of the IoT-cloud combination [71].

Differences in the interpretation of terms partially stem from overgeneral and sometimes vague definitions of CPS systems that include IoT, Industrial internet, Smart cities, Smart grid technologies and comprise digital, analog, physical and human components. As good as this definition may be for general perception of CPS as an enabling technology across multiple fields directly affecting human life, such as health care, emergency response, traffic, and smart grids as noted on the NIST Cyber-Physical Systems website [73], it is somewhat disproportionate in relation to the narrow field of manufacturing process control and belonging ICS.

From the perspective of the automation pyramid based on the ISA-95 model of functional hierarchy, differentiating OT and IT layers, more narrowed definitions would be appropriate for the integration of CPS and IIoT technology into existing architecture.

In that sense, defining CPS as the integration of sensors, embedded computing and networking into physical objects, with feedback loops to monitoring and controlling close physical environments interconnected in a collaborative manner and further connected to the internet [74], would provide a more precise CPS concept and devices used within ICS. Embedded computing implies limited computing capabilities in comparison to the SCADA servers and ICS in general, whereas interconnected physical objects and sensors place Cyber-Physical devices close to the OT layer. Obviously, by increasing computational power and changing their functions respectively, CP devices enter the process control layer and can be considered as the Control-level CPS.

Similar to CPS, industrial IoT is also somewhat broadly defined as a result of relying on general definitions of IoT, which cover a technologically wider area, and refers to consumers IoT that is closely related to consumers electronics that directly affects people's quality of life in their environments varying form smart homes to smart cities [75].

IIoT, roughly defined as a subset of IoT [76], refers to interconnected instruments that can be located on plant floor and in the form of Cyber-Physical devices i.e. smart devices and networked sensors at the OT layer where the real-time communication is the primary concern in communication between sensors, controllers, and gateways [21]. Another kind of IIoT application is implemented at the IT layer, linking together machine learning and data analytics tools that leverage on field IIoT devices, generating data in real time to make analysis accessible locally at the SCADA level as well as remotely via a cloud platform [32].

The above distinction between IoT and IIoT does not mean that typical consumer IoT technology cannot be used in an industrial environment. However, given its characteristics and communication capabilities, which are primarily human-to-machine (H2M), the more appropriate implementation is at the level of the corporate network where the productivity shifts from machine to human actions.

Narrowing the IIoT implementation to the manufacturing industry, Fig. 4 shows the distribution of IoT, IIoT and CPS technology across the ICS networks in relation to H2M and machine-to-machine (M2M) communication and in relation to the SCADA system. Although IIoT is considered a subset of IoT, it has more significant implementation on the process network as opposed to IoT which is more suitable for usage on corporate networks and the internet utilizing H2M communication. The overlap of all three technology concepts within the SCADA system has a consequence of OT and IT convergence partially resulting in disruption of the ISA-95 hierarchical model and forming a more flattened structure that leans toward the I4.0 horizontally interconnected ICS.

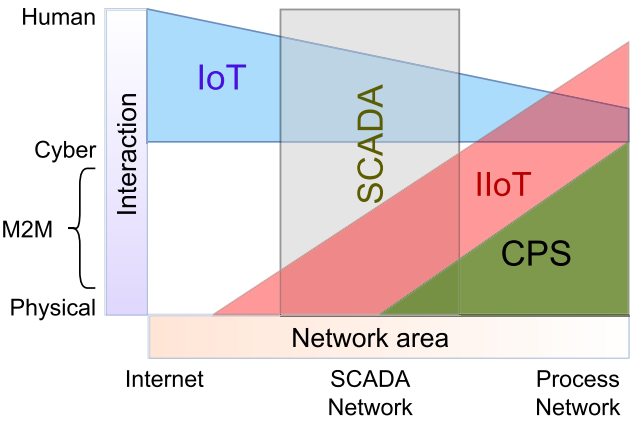


FIGURE 4. IoT/IIoT/CPS Technology distribution across networks, respecting types of interaction.

This can be seen detailed in Fig. 5 which follows the aforementioned concept of CPS and shows IIoT integration in ICS divided into functional layers according to the ISA-95 model. The integration of IIoT devices on the plant floor expands the OT network, whereas the existence of control-level CPS results in IT/OT convergence.

3) SCADA vs. IIoT (IoT)

A third ambiguity arising from the development of ICS driven by new technologies, and thus the evolution of Scada system architecture, is the relationship between IIoT (IoT) and SCADA systems.

The term IoT-SCADA, SCADA-IoT or IoT-based SCADA and SCADA-based IoT for the fourth generation SCADA systems are widely used across industries starting from rather simple cost-effective open source automation and control systems using off-the-shelf components in various domains such as smart home, agriculture, transceiver, photovoltaic stations and others [77], [78], [79], [80] which has the potential to scale to more complex systems for the same purpose [80], to the field of cybersecurity [81], critical infrastructure [57], [82] and risk assessment of such ICS [83].

Although all the above-mentioned works related to IoT-SCADA systems make a clear distinction between these two terms, they also interpret the combination of the same as the integration of technologies into a common control system. Another view, derived from this integration, places

these notions on opposite sides, e.g., SCADA vs. IIoT, and raises the question of whether one will replace the other [84].

In both cases, the SCADA system is determined by hardware and software components and therefore both interpretations can result in a misconception about the SCADA system, and subsequently ICS, which further affects the understanding of architectural structure and functional layers. This can be additionally emphasized at a higher level if the IoT is broadly perceived as an interconnected system of advanced hardware, networks, big data processing and cloud computing, where it can be seen as a layer extending above SCADA and DCS [85]. In this sense, the notion of IoT and SCADA systems needs to be clarified, i.e. the fundamental conceptual differences. As previously stated, if IoT is considered as consumer electronics, i.e. human-centered interconnected smart devices, and IIoT as a network of interconnected sensor-equipped devices with limited hardware, software and energy resources, all of the above strictly implies a hardware component ''thing'' [76]. Such a definition gives a considerable freedom in choice, but it is strict in essence, i.e. in defining the functional boundaries of ''thing'' in IoT or IIoT.

In contrast, the term SCADA is primarily a concept and process, not hardware or software. It is an abbreviation of a strictly functional definition, i.e. performing supervisory control over an industrial process, related data collection and data analysis.

Specifically from an implementation perspective, Stouffer et al. in the NIST special publication 800-82 [86] as SCADA functions state: data acquisition, data presentation and supervisory control (HMI), networked data communication (I/O servers for vendor-specific protocols), alarm and event management, historic data storage (data historian), data trending and reporting.

This definition essentially eliminates any need for comparison of SCADA system with any other physical or cyber-physical and IoT or IIoT devices or concepts, as any IT system performing these functions is a SCADA system in some physical form regardless of its design, structure or architecture.

In this sense, IIoT devices can be integrated into the SCADA system as part of the OT or IT component of an ICS and can independently exchange data through multiple layers of the ICS e.g., the Industrial Internet Reference Architecture (IIRA) cross cutting, but within the current definitional limitations and functionality it cannot independently become a substitute for a concept that includes databases, sets of I/O servers, HMI, IDE, Data historian, virtualization platforms, and has a significant computing power.

C. SERVICES AND IIoT INTEGRATION INTO AUTOMATION PYRAMID

Given the above observations on all three accounts, Fig. 5 provides a general overview of ISA-95 based ICS extended with IIoT and overall shift to the smart factory concept including cloud solutions and services as well as those available on the premises.

The left side shows the automation pyramid derived from the ISA-95 model where the SCADA components are distributed strictly within the L2 layer, interconnected across the IT network and exchanging data over TCP/IP ethernet. The immediate Industrial process control takes place entirely on the L0 and L1 layer containing field devices and standard process control equipment in the form of PLC respectively. Such an architecture is compliant with the addressed SCADA system boundaries, IT/OT division, CPS definition, communication protocols distinction and overall ICS understanding in terms of structure, functionality and interconnection.

With the introduction of IoT/IIoT smart devices, the entire network structure distributed in separated layers and divided by protocols and separated from corporate network, shifts toward a single heterogeneous network resulting in the convergence of process and SCADA networks. Although such an ICS structure can still maintain the functional hierarchy of the ISA-95 model, the SCADA network is significantly influenced by the communication capabilities of IIoT field devices that are able to exchange data across the layers in peer-to-peer communication and directly to the cloud. Additional disruption of the SCADA network within the automation pyramid in Fig. 5 comes from IoT devices at the L1 layer expanding PLC with web server and therefore significantly increasing its communication capability accessing TCP/IP network. These changes not only affect networks and layers, but also the direction of data flow. Observing IIoT field devices residing on the L0 layer, data gathered on the plant floor can be directly exchanged with analytic services (in the cloud or on premises available on the virtual WAN). At the same time, the data generated by legacy field devices and exchanged with the SCADA system via PLC and via ethernet, puts SCADA in the function of a secondary data source to the same analytic services. In this scenario, SCADA acts as a complementary data source for IIoT [87] or vice versa, and therefore disrupts the functional hierarchy where the computational power of the SCADA servers was the predominant factor to determine execution node for computational demanding tasks e.g. data analysis. This scenario gives an example of IIoT integration where the aforementioned definition of IIoT, which implies embedded computing, i.e. limited computing capabilities, does not apply. However, since the ICS expansion of supervisory and process control layers shown on the right side is composed of the self-contained groups of independent functions, these elements are primarily defined as services regardless of their physical form as IoT devices. This approach puts the presented SCADA system in the perspective of a service-oriented smart manufacturing architecture that introduces new computational patterns with on-demand services as the main enabler of value network integration and collaboration, that is conceptually aligned with emerging reference architectures such as RAMI4.0, IIRA, IBM Industry 4.0, and NIST Smart Manufacturing. [88]

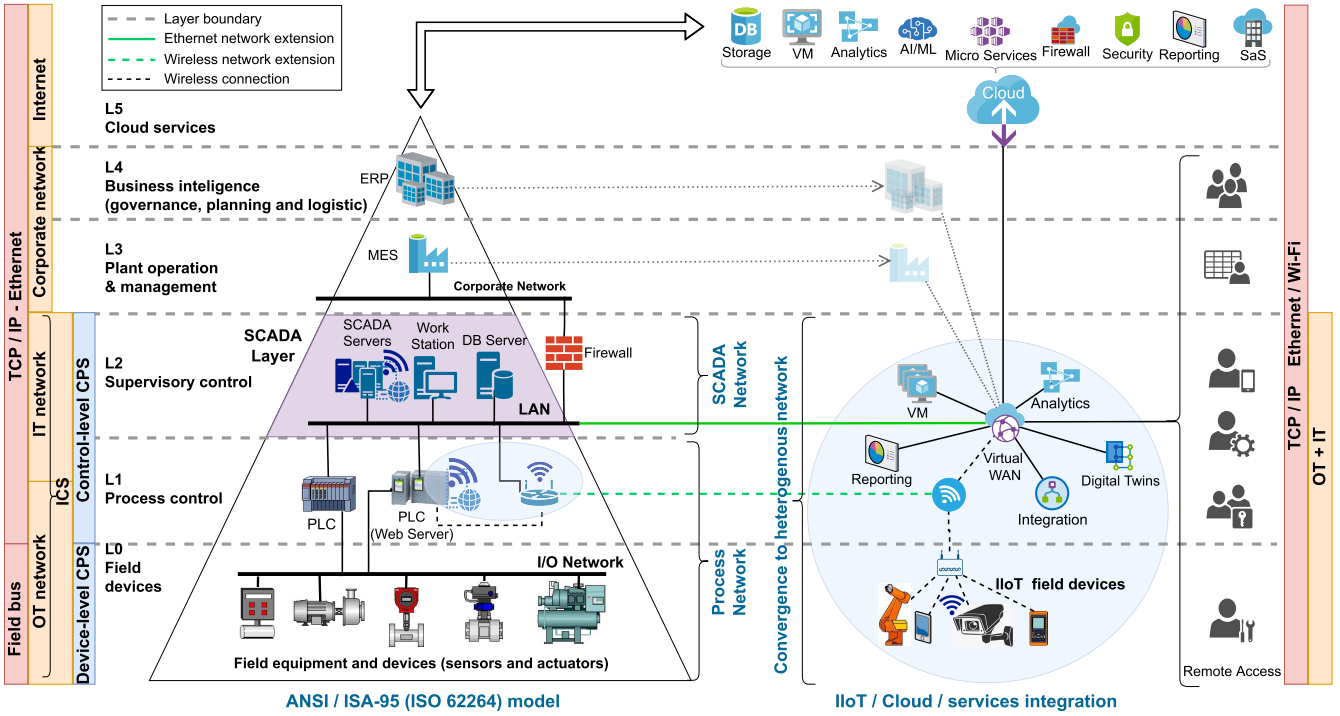


FIGURE 5. IIoT integration into ISA-95 model.

D. ARCHITECTURE REFERENCE MODELS

Despite the general predominant emphasis on interoperability and a high level of integration, ICS systems also become divergent due to the implementation of different communication protocols, technologies, software platforms, custom solutions and system design in general. As a result of such ICS development and the prevailing concepts of I4.0 and the Smart factory, consequently, multiple architectural models have been defined that start from different views of the system. It could be argued that, under these conditions, persistence in defining multiple architectural systems that provide less strictly defined boundaries while increasing a number of layers, elements and different aspects leads to dispersion and does not serve its purpose.

Nonetheless, in conditions where there is an overlap of layers in traditional architectures and cross-layers elements, it is crucial to define a reference model that is flexible enough to include different approaches to ICS and SCADA systems, whereas defining a clear enough framework for future systems development and thus achieving a satisfactory level of standardization that allows easier scalability, integration, interoperability, modularity and increasingly important compliance with security standards, especially in the field of cybersecurity. It is essential that such an architectural model implements multiple aspects and views of the system structure through a multi-layered architecture that encompasses functional, physical, logical, communication, and data views of the system.

1) NATIONAL STRATEGIES AND RESULTING I4.0 REFERENCE MODELS AND FRAMEWORKS

Driven by technological advancement, during the last decade the leading manufacturing countries have introduced several strategies aimed at increasing the competitive advantage of their industries. Table 1 shows chronological order of these strategies and the resulting reference architectures and/or frameworks adopting smart factory concept.

Given the differences in the industrial landscape and national development strategies of individual countries, these reference architectures differ somewhat in focus on the primary domains of interest. In that respect, robotics and interoperability are areas in the focus of Japan's national strategies with a new concept "Society 5.0" prepared by the Ministry of Economy, Trade and Industry (METI) [89]. Additionally, factors such as an aging population and recent impact of the Covid-19 pandemic [90] further emphasize the human component.

In the case of China's industry landscape which is estimated to be outdated with labor-intensive working practices, comparing China's industry automation to the world's leading industries, Kaiser et al. [91] concluded that China's industry is automating differently. Cheaper solutions in partially automated plants and warehouses are being considered instead of progressing towards fully automated production facilities as the world's leading industries are doing. In this regard, China's Ministry of Industry and Information Technology (MIIT) and the Standardization Administration of China (SAC) have released a ten-year national strategy under

the name ''Made in China 2025'' with the intention of transforming the manufacturing industry by providing guidelines to encourage the smart manufacturing applications [92]. One of the resulting projects is the three-dimensional Intelligent Manufacturing System Architecture (IMSA) published in December 2015, which addresses the three key dimensions of system hierarchy, life cycle, and intelligent functions for construction and technology transfer toward intelligent manufacturing systems [93].

The World's Leading position in the IT sector and the importance of the manufacturing sector in the USA resulted in national strategies covered by a framework for revitalizing American manufacturing such as Manufacturing USA (MUSA) [94], the former National Manufacturing Innovation Network (NNMI), established in 2014 [95] and put in motion 2016 [96]. Strategy strongly encourage investment in the creation of new technologies and advocate public-private partnerships to achieve regulatory systems. As a result, several reference architecture models have been defined in the domain of industrial automation.

Based on experience from engagements in manufacturing digitization, IBM industry 4.0 [97] is a commercial architecture derived from use cases developing standard based, modular, plant-specific, vendor-independent and open control systems relying on hybrid cloud models representing a special case of the general Internet of Things reference architecture introduced by IBM earlier in 2017 [98]. It has evolved from its initial two-layer form [88] to its current version by dividing ICS into the Edge, Plant and Enterprise layer, providing an informal detailed overview with an emphasis on communication channels between individual elements as well as between layers. All encompassed elements are described in detail providing communication protocol for each connection within the structure, thus giving a good reference point on the subjects of connectivity and interoperability i.e. communication and integration layers in comparison to other reference models.

Opposed to IBMs Industry 4.0 focus on manufacturing, the Industry IoT Consortium (IIC) provides a more generalized framework applicable across a wide range of industries through IIRA published in 2015 and updated to IIRA v1.9 (volume G1) in 2019 [99]. The four-layer architecture framework is concern-resolution-oriented, i.e. the business, usage, functional and implementation viewpoints of concerns at the input are translated into documented models as architecture representations at the output. This approach addresses stakeholders, business vision, value and objectives of the entire IIoT system as well as the interaction and interconnection technologies to implement functional components and their life-cycle procedures in an iterative process. The intention is to provide generic methods and templates for the development of widely applicable industrial IoT control systems with minimal architectural constraints, i.e. concrete technologies or standard specifications.

Introduced in February 2016 by NIST in the document Current standards landscape for Smart manufacturing systems [4], The Smart Manufacturing Ecosystem (SME) provides a model for the existing manufacturing standards landscape classification in relation to ecosystem dimensions (product, production, enterprise-business) and a method for grouping the standards according to functions defined alongside each dimension. These three dimensions of concern are presented as a sequence of functions necessary to fulfill the life cycle of each dimension with the purpose of achieving corporate competitive objectives by addressing smart manufacturing capabilities defined as productivity, agility, quality and sustainability. The core of the system is the intersection of all three dimensions in the manufacturing pyramid as a central point of convergence and interaction achieving vertical integration according to ISA-95 functional layers.

Li et al. [56] observe that ecosystem architecture only describes ICT application systems and notice that improvement of the enterprise infrastructure cannot be found in the architecture which excludes cloud, big data, IoT, CPS, digital twins and other I4.0-related technologies. In their conclusion, NIST's smart manufacturing standardization is considered to be suitable primarily in the field of application.

This conclusion is justified considering that SME relies on the manufacturing pyramid whose vertical structure is not consistent with typical I4.0 convergence of the OT and IT layers. Nevertheless, even if manufacturing standards landscape classification is built on top of such defined dimensions, it presents a valuable starting point for ICS transition toward smart manufacturing concept.

2) GERMAN INITIATIVE AND RAMI4.0

In contrast to the multiple initiatives and resulting architectural models introduced by various reference institutions and companies in the USA, in April 2013 the German government, acting through the Ministry of Education and Research (BMBF) and the Ministry of Economic Affairs and Energy (BMWI), published a national strategy Industrie 4.0 [100] with recommendation for implementation [101], which led to a unique but comprehensive and widely accepted RAMI4.0 [8] leveraging key concepts of the Internet of Things and Services (IoTS), CPS, and smart manufacturing with in depth focus on production scenarios, connectivity, integration, value stream and life cycle management relying on existing IEC 62264 [102], IEC 62890 [103], IEC 61512 [104] standards and setting new pre-norm IEC PAS 63088 [105]. The idea of RAMI4.0 is not a specific architecture definition but rather a minimum requirement framework for the class of architectures to be modeled [106]. Such an approach allows a gradual migration from legacy industrial plants to smart factories relying on broadly accepted standards. The key elements for the realization of this flexible implementation of the architecture model are the semantic interoperability achieved by virtual representation of I4.0 components (via asset administration shell), ''*type*'' and ''*instance*'' through which life cycles and value streams are addressed.

The Visual presentation of the complex and comprehensive I4.0 concept of diverse viewpoints is simplified into a three-dimensional form that describes the fundamental aspects of I4.0 across three axes and six layers. Whereas the right horizontal axis relies on the ISA 88/95 technical report [107], IEC 61512 and IEC 62264 standard of functional hierarchy expanded with "*product*" at the bottom level and "connected world" at the top level exceeding plant facility boundaries, the left horizontal axis relies on the IEC 62890 standard and represents life cycles with associated value streams followed by continuous data acquisition enabling rapid and dynamic response to demand changes [76]. Within the life cycle of a product or system, there is a clear distinction between the development and use stages. While the product is in the planning, design and development phases, it is considered to be a "*type*" that has its own life cycle segment (design, maintenance, usage). Once a product is ready for production, it becomes an "*instance*" of a type with a unique identifier and a life cycle (production, maintenance, usage) that continues to be tracked by data collection throughout the full extent of its lifespan. Whether a product is considered to be a type or an instance depends on the position of the individual stakeholder, i.e. entry point in the system. The vertical axis contains six layers (businesses, functional, information, communication, integration, asset) which present the decomposition to various perspectives and thus form an IT representation of an manageable I4.0 component. More specifically, these six layers address communication behavior, virtual presentation of hardware/software entities, business process, functional descriptions, protocols, data formats, transmission, formal definitions of functions, data processing and integration, data mapping etc. According to the goals and advantages of RAMI 4.0 introduced by the working group on reference architectures, standards and norms [108], the second dimension, i.e. the layers, should provide answers to the following questions:

- Asset: how to integrate the product (hardware, software, documents) with the industrial process and to progress in the real world from a development and utilization perspective considering the entry point of the product into the system from the point of view of individual stakeholders.
- Integration: which elements of the asset are, or may become, digitally available on the network respecting the product life cycle.
- Communication: how will the users in their respective roles (operator, developer, customer, designer, management) access data in a uniform way and at any point of the product life cycle.
- Information: what information about the asset can be provided relevant to the industrial process or the asset/product itself.
- Functions: what are the specific rules and functions defined for the process/product in question, i.e. what is it supposed to do.
- Business: what is the added value from the commercial perspective.

From the perspective of interoperability and connectivity as the enabling forces of I4.0 in the core process of physical to digital conversion, the initial and crucial transformation takes place at the Asset layer as the entry point for the digitalization of any hardware or software element of concern. The asset layer defines basic elements with communication capability placed in relation to other elements in the form of uniquely identified objects in order to make their data available across the network.

In accordance with the digital factory framework IEC 62832 standard [109], an asset is defined as a managed physical or logical object whose properties can be accessed through the administration shell with which it is uniquely related and thus forms Industrie 4.0 component. The basic structure of the Asset Administration Shell (AAS) is roughly divided into a header that contains identifying details and a body containing submodels as structured asset-specific properties that can refer to data and functions in a standardized format based on the IEC 61360 common data dictionary. Thus defined, domain-specific submodels i.e. manifest of the asset administration is constantly available via interaction manager residing within the administration shell stored in the asset or in a database [110] and enabling interaction patterns in standardized data exchange, achieving semantic interoperability through the entire asset and instance life cycle, i.e. from design and construction through commissioning to operation and maintenance [85] as one of the Industry 4.0 core objectives. Another intention behind the administration shell is to accelerate the implementation of non-proprietary solutions as part of the I4.0 network [8], which is additionally facilitated in the part two of administration shell specification [111] by introducing technology neutral specification of the application programming interface (API) available in different technologies such as HTTP/REST, MQTT and Open Platform Communications United Architecture (OPC UA).

3) GLOBAL IMPACT AND PREVAILING REFERENCE ARCHITECTURE MODELS

The reference architecture models have been developed as a result of recognizing the global phenomenon of disruptive technology potential in implementation across industry sectors, and within the boundaries of national strategies and initiatives addressing the fourth industrial revolution. As such, even if they are not domain-oriented, they inevitably reflect the national industry landscape and domains of strategic interest. However, recent technological advancement, followed by international industry standards, have global impact and cannot be reduced to isolated national frameworks, nor should any architectural model strive for an isolated ecosystem. The harmonization of existing reference architectures on a global scale is imposed as a practical long-term solution.

Addressing the state of the art and future trends of Industry 4.0 reference architectures, Nakagawa et al. [112] have

pointed out the popularity of RAMI4.0 and IIRA, whose appearance in scientific work is over ten times more frequent in comparison to other relevant architectures in their research. According to another research conducted by Bader, Maleshkova and Lohmann [113], IIC and Platform I4.0 ranks in the top three IIoT reference frameworks ranked by Google scholar in terms of research relevance. This alone is not absolute proof of the international level of acceptance, but it is significant in identifying current and future development trends led by the scientific community that potentially result with new international standards that reaffirm these two reference models at a global scale.

Two key factors for global acceptance are present in the concept of these two reference architecture models: 1) Both models address the cutting edge of advanced technologies and concepts of concern for the world's leading innovation-oriented industries, leading to a short time to implementation providing current use cases, and thus accelerates standardization and increases acceptance rate. Furthermore, it paves the way for the future development of industries that currently follow a different approach, as it is the case with China [91]. 2) International collaboration between IIC and Platform I4.0, that began in 2015 in the early stages of architectural model development and resulted in architecture alignment and interoperability, thus ensuring a comprehensive model for wider acceptance.

In the case of RAMI 4.0, international cooperation and harmonization of architectural models was the approach from the very beginning by defining the structure of the administration shell through trilateral cooperation of Italy, France and Germany, i.e. their national initiatives Piano nazionale impresa 4.0, Alliance industrie du futur and Plattform Industrie 4.0, respectively [114]. Furthermore, the work of the Sino-German Standardization cooperation commission has resulted in alignment with China Intelligent manufacturing system architecture (IMSA), originally formed in November 2016 [115]. Between 2016 and 2020, the German-Japanese cooperation for the standardization of Industry 4.0 and the Industrial internet of things formed three work groups focusing on standardization (use cases and applications), digital business models and cyber and industrial security [116] under the common strategy for I4.0 and IIoT [117].

E. THE IMPORTANCE OF THE REFERENCE ARCHITECTURE MODEL FOR THE EVOLUTION OF ICS AND SCADA SYSTEMS WITHIN CONTINUOUS PRODUCTION FACILITIES

When it comes to ICS, and thus the SCADA system, the reference architecture is, among other things, important for the transition from legacy ICS to the smart factory concept, i.e. cloud, IIoT and service-oriented SCADA system. ICS systems do not upgrade or get replaced unless there is a valid and obvious reason to do so. Industrial production facilities, and particularly the continuous production process that runs continuously 24 hours a day, does not stop if the reason for the downtime is not a breakdown or planned maintenance. Every other production interruption, especially multi-day ones, must justify not only the overhead costs, but also the lost profits caused by the cessation of production, which in the case of the production process in Fig. 2 can reach millions of dollars per day. If the reason for the shutdown is a replacement or a major upgrade of the ICS system, the new system must justify the time spent, which may ultimately exceed the cost of the ICS system itself.

Similarly, providing an overview and background of Industry 4.0 concept, and addressing the current state of industry, Rojko [118] has drawn attention to the following basic prerequisites that must be met to facilitate the transition of the industrial production system to the new smart factory concept:

- Stability of the production process in the transition phase must be guaranteed.
- Gradual approach to the transition due to significant financial investment is necessary for major technology transfer.
- Know-how protection is necessary (extending to the cybersecurity domain).

Following Industry 4.0 concept introduction, in October 2015 The Cologne Institute for Economic Research and Aachen University [119] published results of a more comprehensive analysis of the readiness of the German companies for transition to Industry 4.0, applying evaluation model with the following six dimensions:

- Strategy and organization (investments, innovation management).
- Smart factory (digital modeling, equipment infrastructure, data usage, IT systems).
- Smart operations (cloud usage, IT security, autonomous processes, information sharing).
- Smart products (data analytics in usage phase, ICT add-on functionalities).
- Data-driven services (share of revenues, share of data used).
- Employees (employee skill set, skill acquisition).

The study was conducted on 268 mechanical and plant engineering companies and showed that 56.5% of all companies covered by the survey do not meet any requirements of concern to implement Industry 4.0 concept, and only 0.3% of companies have sufficiently addressed all six dimensions of the evaluation model.

For these reasons, most manufacturing facilities associated with continuous and expensive industrial processes such as the steel industry, continue to operate on legacy ICS, with upgrades occurring in micro-phases as part of regular maintenance cycles. Exceptions to this practice are usually the following cases: 1) Revamping of the entire plant or major part of the equipment, usually with the aim of improving the overall control of the production process, for which the existing control system has become inadequate; 2) Outdated ICS with known security risks that may directly or indirectly affect the stability of production; 3) Implementation of a new function, i.e. addition of software/hardware to existing ICS,

TABLE 1. Digital/smart manufacturing strategies and reference architecture models.

Year	Country	Regulatory body	Initiative/ defining doc.	Proposed Architecture	Description and Purpose
2011	EU	SFP[a]	IoT–A[b]	IoT–ARM[c]	Interoperability at the communication and service level for building IoT-based solutions in compliance to the IoT reference model and guidelines (forming three constitutive parts of IoT-A), which leads to faster development and gives different views and perspectives of concern to stakeholders.
2015	China	MIIT[d], SAC[e]	Made in China 2025	IMSA[f]	Defines manufacturing system elements and attributes through interconnected entities encompassed by the three-dimensional series of system hierarchy, Intelligent characteristics and Life cycle. The purpose of such decomposition is to establish an advanced manufacturing standardization architecture and provide a development framework focused on IT integration in industrial processes.
2015	USA	IIC[g]	IIC:PUB: G1:V1.80	IIRA[h] Vol.G1	Guidance for system architects, integrators and users in form of an architectural template to define IoT systems focusing on the OT/IT convergence. The usage of IIRA aims to achieve consistency in implementation across different industrial sectors providing a common platform for general understanding among stakeholders of different viewpoints (business, usage, functional, implementation), and raising the level of interoperability between different systems deployed under the same architecture.
2015	Germany	DKE[i], ZVEI[j], DIN[k]	Industry 4.0	RAMI 4.0[l]	An orientation framework proposing a three-dimensional and six-layer structure that provides a detailed model for the smart manufacturing value chain through the concept of I4.0 components, horizontal and vertical integration, administrative shell, hierarchy levels, data flow, and associated value streams. The purpose of the such architecture is to provide flexible methods and relevant standards for easy and reliable integration of products, parts and devices into the service-oriented environment of Industry 4.0
2015	Japan	IVI[m]	IVC[n]	IVRA[o]	Provides a structure for manufacturing Industrys through three views (Activity, Asset, Management) in compliance to smart manufacturing concept aligned with Japanese industry trends and based on loose and adaptive standards with focus on "Connected Factories" and "Connected Workplaces".
2016	USA	NIST[p]	NISTIR[q] 8107	SME[r]	Clarifies the concept of smart manufacturing through the three vectors of concern (business, product and production). Each vector is formed as a set of existing standards and has its own life cycle that includes the appropriate structural elements, data flow, functions and interactions. All three vectors rely on the ISA-95 based manufacturing pyramid.
2017	USA	IBM	I4.0	Industry 4.0 RA (IoT RA)[s]	Constructs three-layers (edge, plant, enterprise) consistent logical architecture resilient to changes in the physical context with the intention of providing flexibility of deployment and functionality shift across layers to meet case-specific requirements. The architecture is significant in assumption of the close deployment environment with an emphasis on autonomous operations, connectivity, data access, privacy, security and OT/IT convergence within the manufacturing environment.
2017	USA-Germany	IIC/I4.0	IIC/I4.0	IIRA/RAMI4.0	Architecture alignment of complementary elements of IIRA and RAMI4.0 reaching for interoperability in the domain of manufacturing industry by combining broad applicability of IIoT technical frameworks in multiple Industrys provided by IIRA with digital transformation of entire value chains and product life cycles encompassed by RAMI4.0. In its current form, it provides a model for interoperability within IIoT systems on complementary layers of connectivity and communications.
2017	Germany-Japan	PI4.0[t] RRI[u] SCI4.0[v]	CSIIoT/I4.O[w]	URM–MM[x]	A procedural guide that aims to facilitate the use of available reference architectures, standards, initiatives, concepts and methods for each specific use case with a four-step system definition (Canvas, Use-case, Function, Data) to link the relevant international standard to the described system. This mapping methodology is a navigation tool for the development and technological transition of individual use cases towards smart manufacturing systems.
2018	Japan	IVI	IVC	IVRA-Next	Extended IVRA to adopt IoT and deliver a grand design for connected manufacturing.
2019	Japan	IVI	IVC	CIOF[y]	Data utilization and data flow/distribution cross-platform mechanism within "Connected Manufacturing" in order to achieve more flexible and efficient business.

[a] SFP: Seventh Framework Program founded by European Commission, [b] IoT-A: Internet of Things – Architecture, [c] IoT-ARM: Internet of Things – Architecture Reference Model, [d] MIIT: Ministry of Industry and Information technology of China, [e] SAC: Standardization Administration of China, [f] IMSA: Intelligent manufacturing System Architecture, [g] IIC: Industrial Internet Consortium, [h] IIRA: Industrial Internet Reference Architecture, [i] DKE: Association for Electrical, Electronic and Information Technologies of DIN and VDE, [j] ZVEI: German Electrical and Electronic Manufacturers Association, [k] DIN: German Institute for Standardization (DIN Deutsches Institut für Normung), [l] RAMI 4.0: Reference Architectural Model Industry 4.0, [m] IVI: Industrial Value Chain Initiative, [n] IVC: Industrial Value Chain, [o] IVRA: Industrial Value Chain Reference Architecture, [p] NIST: National Institute of Standards and Technology, [q] NISTIR: National Institute of Standard and Technology Interagency Report, [r] SME: Smart Manufactoring Ecosystem, [s] Industry 4.0 RA: IBM Internet of Things Industry 4.0 reference architecture, [t] PI4.0: Platform Inustrie 4.0, [u] RRI: Robot Revolution Initiative, [v] SCI4.0: Standardization Council Industry 4.0 [w] CS IIoT/I4.O: Common Strategy on International Standardization in Field of the Internet of Things/Industry 4.0, [x] URM–MM: Unified Reference Model–Map and Methodology, [y] CIOF: Connected Industrys Open Framework,

resulting in improved process control and/or final product; 4) Disrupted supply chain resulting in ICS critical spare parts being unavailable (depending on locally available services, support or spare parts, this instance can be addressed within the regular maintenance cycle).

Regardless of which of the above cases the transition of the overall ICS or only SCADA system is carried out, it is a continuous iterative process that takes place in phases. It is important that the ICS system, in any of its parts, changes in accordance with a clear vision of the direction of development and the general picture of the final form of the system. At the same time, it is to be expected that the vision and final shape of the system will change over time in several potential directions, which may not be consistent with any architectural model. In this sense, an important role in the construction, maintenance and expansion of ICS has a reference model that is flexible enough, i.e. capable of covering multiple system development scenarios and providing a comprehensive concept within which all system levels can be defined. A system built in this way can remain relevant for a longer period of time, and be flexible enough to implement technologies that are yet to come within the existing framework.

F. ARCHITECTURAL MODELS SIGNIFICANT TO SCADA SYSTEMS AND STEEL INDUSTRY DOMAIN

Although all the reference architecture models listed in table 1 are related to Smart factory and aim to facilitate the development of ICS, they do not have the same significance and impact on SCADA systems when it comes to the continuous production processes in the metal industry for several reasons:

1) Most of the existing SCADA systems in the metal industry belong to 2nd and 3rd generation, and have only been partially developed with 4th generation-specific elements maintaining the ISA-95 structure. In this regard, each use case is very specific and implements only part of the smart manufacturing concept. For such cases, URM-MM provides a mapping methodology for cross architecture elements in accordance with existing standards, and therefore better suits a particular use case scenario than any reference architecture in particular.
2) The specificities of the continuous production process are reflected in the design and control system requirements and may exceed the capabilities of the reference frameworks generally applicable to multiple industries, such as healthcare, transportation and public domain. For an appropriate approach to the development of ICS and SCADA systems applied in the steel industry, especially when building a new system, a better orientation would be achieved by a reference architecture with an in-depth orientation to the manufacturing industry such as RAMI4.0.
3) In the area of the steel industry, in the communication with the OT layer, SCADA systems are primarily based on proprietary protocols. With the introduction of IIoT technologies and I4.0 concepts, where the protocol map changes significantly due to IT / OT convergence, the key importance in the implementation of the reference architecture lies in communication and integration layers, which is the strong point of IIRA / RAMI4.0 architecture alignment.
4) Steel manufacturing plants are relatively independent systems and with a rather low level of human interaction. In this regard, reference architectures such as Japanese IVRA focusing on the national strategy of "*Connected Factories*" and "*Connected Workplaces*" would not provide satisfactory results.
5) In the domain of steel manufacturing, SCADA systems tend to become complex structures due to the process control requirements, interconnection of different control systems, overlapping of distributed and centralized functions and other previously addressed industry-specific requirements. Taking this into account, SCADA system development process, maintenance and further evolution during its life cycle would benefit from a decomposition providing clear separation of functions, integration mechanisms, communication protocols, data acquisition and interpretation models with the resulting information on which functions to leverage in control of industrial processes. Considering that data, information, internal rules and functions are plant specific, and to some extent case-specific as well, it is crucial that the architecture model provides a framework for such decomposition, which RAMI 4.0 does in three dimensions.

With these considerations in mind, Fig. 6 shows the SCADA component of ICS, transferred to the three-dimensional structure of the RAMI 4.0 reference model. The ICS example is taken from the previously shown extension of the ISA-95 structure with IIoT components in the service-oriented structure of the Smart factory concept. In order to avoid confusion in the display of the three-dimensional structure, only the elements sufficient to understand the structure and display the decomposition of the SCADA system through the layers are transferred. The hierarchy levels on the right axis follow the IEC 62264 standard, which means that the automation pyramid can be functionally translated into one of the three dimensions of the RAMI 4.0 model. In doing so, the Product level does not play a significant role from the SCADA point of view, given the characteristics of the product in steel manufacturing, which is one-dimensional and passive, i.e. the possibilities of life cycle monitoring at the level of the product itself are extremely limited. Since the RAMI4.0 model is in depth oriented to the manufacturing industry, the left axis follows the life cycle through all hierarchy levels involving development (Type) and production (Instance) i.e. usage. In Fig. 6a, the emphasis is on showing the structure of the SCADA system in operation, thus emphasizing the right side of the left axis, i.e. the Instance.

Looking at the vertical axis, the following can be observed across the layers: **Asset layer** represents the real-world physical and software components where the field devices and SCADA software life cycle, i.e. value streams, are shown. The *Software product*, developed from functional specifications, documents and algorithms along the axis at the station level, is further transferred to the PLC and SCADA server located at the control and station levels of the integration layer. This one-to-many relation is possible due to the integrated development model in which PLC and HMI/SCADA software share the same IDE, e.g. the Siemens TIA portal. Accordingly, physical devices are developed along the field device level and digitized at the Integration layer by AAS.

Integration layer performs the acquisition and digitization of information from the industrial process, i.e. connects it with computer-aided control, which includes a major part of the traditional SCADA system. This is where a digital image of the physical process is created, leveraging on AAS that enables I4.0 compliant in-layer communication between field devices and IT equipment. In this example, the virtual representations of the plant devices exchange data with each other in a direct connection that further extends to the PLC and SCADA server (control and station levels) via router, using the communication protocols available at the communication layer. Although this example works well in case of I4.0 component integration, legacy field devices using various proprietary protocols cannot benefit from this arrangement which presents a barrier for 2nd or 3rd generation SCADA systems that gradually implements IoT and progress to the I4.0 concept with field devices that do not comply with I4.0 components.

As OPC UA is the preferred communication standard for RAMI 4.0 [114], [120], it is prevalent in I4.0-related case studies and proof of concepts [121], [122], [123]. However, addressing the problem of existing fieldbus protocols, an AAS containing an OPC UA Server according to the IEC 61131–3 specification was proposed in [123], whereas Seif, Toro and Akhtar [124] presented a use case of AAS modeling to adopt devices that are not compliant with the I4.0 component by parsing a comma-separated file (containing the device definition and characterization) and creating a submodel serialized in JSON (or XML) format. They also recognize the benefit of using an IoT platform with a smart gateway able to map device-specific data from various low-level protocols. In approach to hybrid cloud architecture for AAS, Bauer and Makio [125] proposed administration shells conceptualized around the usage of the Actor Model, applicable in the area of edge and cloud computing. Devices become OPC UA ready by interconnecting assets that contain an additional hardware module acting as a gateway. This modification extends AAS to a gateway that provides protocol conversion for legacy field devices. This may seem unnecessary since these field devices already have an existing communication channel with the PLC via the fieldbus protocols, but this way these devices become IIoT enabled and therefore a valuable data source horizontally interconnected within ICS SoA. Additionally, using the same principle, the integration of individual elements from other control systems of significance is possible as well, e.g. direct measurements reading from devices located on the SAS communicating over the IEC 61850 standard protocol. Such a model of AAS connection with physical assets in the form of legacy field devices enhanced with smart gateway as a protocol converter is depicted in Fig. 6.

In addition to the virtualization of physical devices through ASS, and consequently, monitored physical process, another concept of virtualization is evident at the station level in the form of type1 or type 2 hypervisors, i.e. virtual machines on SCADA servers that provide a virtual environment for HMI server-client systems and servers redundancy. Although this, when implemented, is a key segment of the SCADA system, from the perspective of reference architecture it should be considered as a black-box, i.e. its functionality should be accepted as a service at the hardware and software level without the need for further decomposition or standardization.

Communication layer standardizes communication using a uniform data format and provides services and mechanisms for data transmission (interfaces, communication channels, ports, data providers, protocols), harmonizing communication toward Information layer, while simultaneously enabling direct communication over the real-time network for time sensitive applications [126]. Although all components are interconnected at the Integration layer, the actual communication is enabled by the Communication layer. In this instance, components at the Integration layer are associated with the appropriate protocols used in the interactions of IT components and edge devices with the interconnected AAS. The Communication layer, shown as part of the RAMI 4.0 structure in Fig. 6, contains only the protocols used by I4.0 component compliant field devices according to the AAS specification part2 [127]. If an AAS, communicating via the smart gateway shown in Fig. 6, were to be used, the Communication layer would be significantly expanded with supported fieldbus protocols.

Information layer is concerned with the processing and integration of collected data. It provides a general virtual representation of I4.0 component's individual meta-data, such as the AAS manifests, and any information related to real-time data acquisition or controlled process rules-related information, thus acting as a key link between data gathered at the Integration layer and decisions made as a consequence of the data interpretation, i.e. information. Industrie 4.0 compliant communication is therefore a crucial precondition in the Integration layer in order to provide relevant information at a higher level here.

Function layer describes the functions and services necessary for the decision-making logical process, i.e process capabilities. This is where the application runtime environment (HMI, reporting, analytics, client interfaces) is executed. All available functions are plant-related, i.e. derived from each individual industrial process controlled by a dedicated ICS. To ensure the integrity of the information provided along with integration at the technical level, remote access and horizontal

integration are only available at this layer. According to [8], the Asset layer and the Integration layer can be accessed from the Function layer for direct communication to devices (requesting diagnostic data, or trigger device-related calibration sequence). This is an exception to the RAMI 4.0 communication pattern, where each layer is interconnected and communicates only with adjacent layers. However, this is considered a temporary connection for maintenance purposes only, and is not relevant for permanent horizontal integration.

G. REFERENCE ARCHITECTURE STANDARDS

Despite the high level of integration and interconnectivity that extends to cloud-based and service-oriented solutions, resulting in overall convergence and thus flattening out the traditional automation pyramid, the IEC 62264 standard remains the starting point, i.e. the common ground for standard-based (RAMI4.0, IIRA, IMSA, SME) and empirical (IBM) architectures. Weather it is implemented in only one layer, as in the RAMI4.0 Asset layer, or it takes the central point in the cross-sections of dimensions as in SME. ANSI/ISA-95, the reference point of IEC 62264 standard is primarily a functional hierarchy, which makes it relevant for understanding the core of ICS functionality, elements, and thus the structure of the SCADA system with associated standards distributed through the functional layers of the manufacturing pyramid [128], [129].

Table 2 contains existing standards to which reference architectures are associated, and the new standards defined by addressed reference architectures. Given the wide range of different industry domain-related standards implemented by the reference architectures, they are not entirely a reflection of the I4.0 concept, and thus not of the 4th generation of SCADA systems as well. They are rather the result of attempts to cover multiple fields of implementation by encompassing broader domain-related norms, frameworks and existing solutions. To provide a clear comparison of implementation against reference architectures, we have excluded domain-specific automation standards such as IEC 61672-2, ISO/IEC 12812-1, ASME Y14-5. In addition, the publication years of the standards in Table 2 have been reduced to the most significant period of eight years (2015 – 2022) given the time span in which the majority of reference architectures were defined in accordance with data in Table 1, and established globally through multilateral initiatives, aimed at reference architecture alignments.

The following relations to standards are considered: 1) Existing standards with which the architectures are explicitly compliant. Although this does not cover all the standards to which a particular reference architecture is compliant with, they are documented in the official documentation and research papers related to the respective architectures, e.g. Asset Administration Shell (AAS) of RMI4.0 [130]. 2) New standards defined by reference architectures. These are the standards such as ISO/IEC 30141 and IEC-PAS-63088, which are, in fact, the definition of the respective architectures or one of their inner components, as in the case of IEC 63278, which defines AAS within RAMI4.0. These standards are essentially a subset of the previous set of standards. 3) Standards that reference architectures implicitly apply, i.e. they are implied with regard to specific areas of application, e.g. data interoperability, asset management, production engineering, etc., although not explicitly stated in the official documentation of the relevant regulatory body.

In the comparison between the reference architectures there is alignment in compliance with the standards explicitly related to the IoT, communication, data model and integration (IEC 62601, IEC 62541, IEC 62591, IEC 62657, IEC 61784-2, ISO/IEC 30161, IEC 20924) as a result of the common research interest of all addressed reference architectures. Furthermore, looking at the Edition column, 17 new standards have been defined (two of which are under development), including five groups of standards, which makes the total of over 50% of the covered standards. Although the data in Table 2 are rather indicative, this is a good indication of the effort invested in regulating the design of the next generation of industrial automation systems that paves the way for further concrete guidelines on how to design, implement, operate and maintain SCADA systems, such is the work of the ISA112 SCADA Systems standards committee [131].

1) LOOSE STANDARD APPROACH AND PROCEDURAL GUIDELINES

The reference architectures RAMI4.0 and SME generate most of the standards in the table as they are architectural frameworks that have emerged from the initiatives focusing on alignment and international standardization in the field of IoT and I4.0, i.e. Smart manufacturing [114], [115], [116], [132], [133], [134] through cooperation between standardization committees and national strategies [95], [96], [117], [135].

Alternatively, the Japanese approach through the IVRA (IVRA-next) reference architecture [136], [137] seeks to achieve an ecosystem of interconnected manufacturing enterprises throughout the value chain. Following the concept of loosely defined standards (LDS), IVRA is not based on a predefined set of national or international standards, but rather seeks to achieve a common ground for interfacing unique entities through a scenario-based set of rules for entity-to-entity connection [138]. This concept strictly implements only data model standards to provide a basis for system integration, whereas the implementation of available integration methods, techniques and components as off-the-shelf solutions [139] developed by numerous advanced study groups (ASG) [140] is subject to change. In this way, data and the consequent knowledge are available throughout the network of digital twins among companies with loosely defined components and structure [141].

Similarly, a collaboration between Germany and Japan introduced the URM MM, which can be considered a continuation of the IVI approach in the form of a procedural guide that enables stakeholders to navigate relevant international standards and available reference architectures from

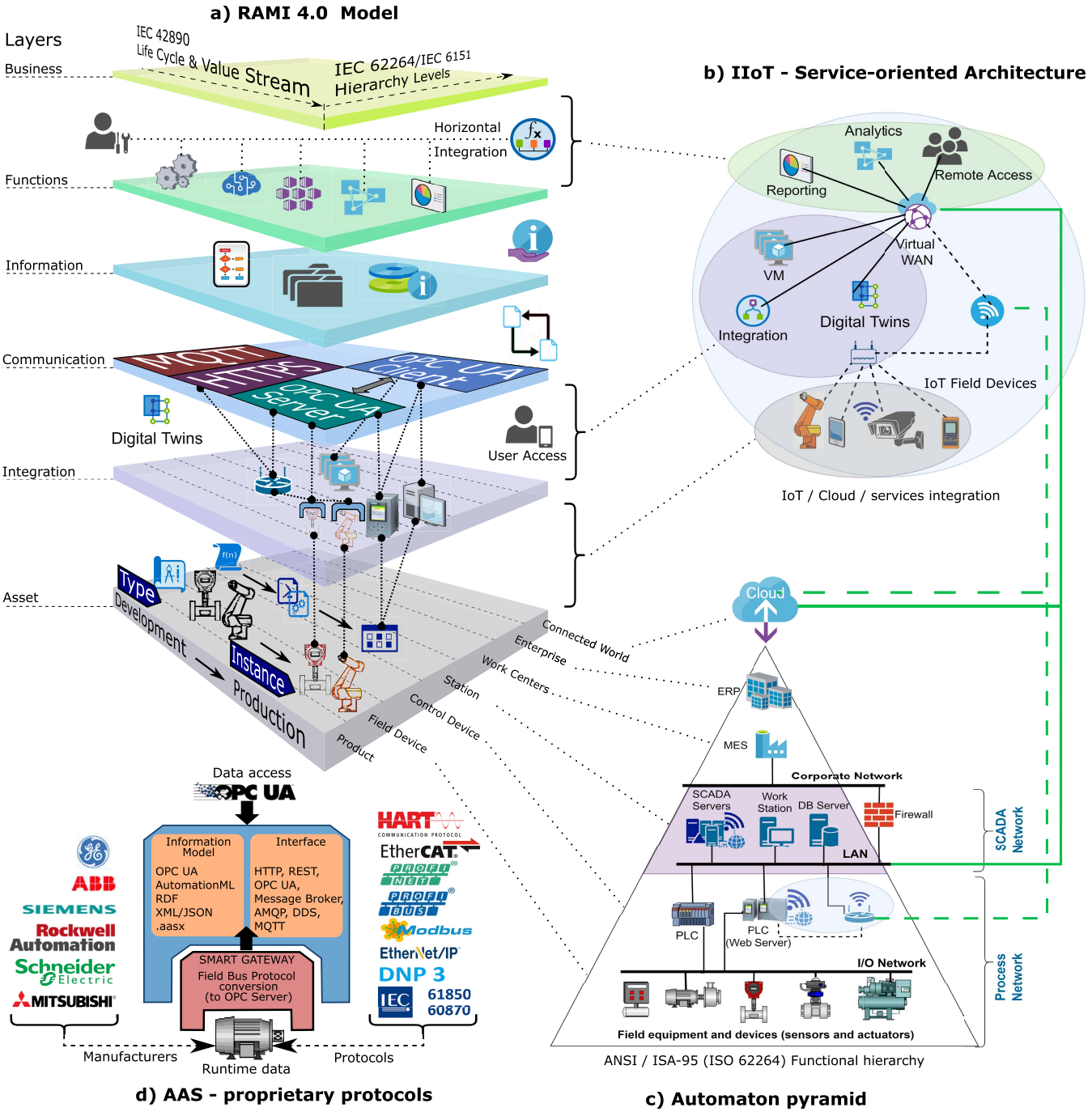


FIGURE 6. 3rd generation SCADA System in transition to IIoT/Services integration, presented in RAMI4.0 3D structure.

pre-categorized models to address specific use cases for each development process [132]. The URM MM column in Table 2 includes the standards referenced through the Canvas, Use case, Function and Data phases of URM MM [142], [143]. Although these international standards are explicitly stated in the cited paper [142], the relationship is marked as implicit due to the concept of URM MM, i.e. relying on the use of existing predefined models. For the same reason, basic communication and IoT-related standards are not marked because it is expected that the predefined models used are already compliant. Principles similar to LDS can be found in the European IoT-ARM, resulting from the IoT-A project based on the current state of the art, rather than using a clean-slate approach [144]. This kind of approach is therefore orientated towards in-depth analysis that has been methodologically conducted on existing concepts and solutions in the domain of connectivity [13], [145], Orchestration of distributed IoT services [146] and security [147].

In this regard, IoT-ARM does not explicitly implement international standards. Instead, they are inevitably included through the implementation of existing and well-known approaches of views and perspectives that IoT-A follows [148]. To facilitate navigation through them, a Unified requirement list [149] has been introduced to map to the corresponding views and perspectives from the reference model. Each requirement in the list consists of a unique identifier, requirement type, category, description, rationale, view, perspective, functionality group, functional component and domain model. The purpose of such a dynamic table is to assign each requirement to the components of the reference model in a standardized way, and therefore has the role of IoT-ARM internal standard.

2) LOCAL STANDARDS PREVALENCE

An exception within the standard-oriented reference architectures is the Chinese national strategy and the corresponding IMSA, which, despite the implementation of the global I4.0 paradigm, is oriented toward national standards. To define the reference architectures, standards and guidelines for smart manufacturing, in February 2015 the Department of Equipment Industry within the Ministry of Industry and Information Technology (MIIT) established a working group whose technical committees include four main institutions: Information Technology of Standardization Administration of China (TC28), China National Technical Committee for Automation Systems and Integration Standardization (TC159), Industrial Process Measurement and Control of Standardization Administration of China (TC124) and China's National Information Security Standards Technical Committee TC(260) [150]. According to an update of the five-year plan published in February 2021, a total of 285 national standards related to the manufacturing industry have been published [151]. Furthermore, the Guidelines for construction of a national smart manufacturing standards system [152] aim to define and revise more than 100 national smart manufacturing standards by 2023, structured in three parts:

- A Foundational and general purpose: general purpose, security, reliability, testing, evaluation, Personnel capabilities)
- B Key technical:
  - BA Smart equipment (additive manufacturing equipment, inspection and testing equipment, human-computer collaboration systems, CNC machines, industrial robots, processing equipment, other)
  - BC Smart supply chains (supply chain construction, supply chain management, supply chain evaluation).
  - BD Smart services (mass customization, O&M services, networked collaborative manufacturing).
  - BE Intelligent enabling technology (artificial intelligence, industrial big data, industrial software, industrial cloud, edge computing, digital twins, blockchain).
  - BF Industrial networks: industrial wireless networks, industrial wired networks, industrial network convergence, industrial network resource management.
- C Industry application (shipping and marine engineering equipment, building materials, petrochemical, textiles, iron and steel, rail transportation, aerospace, nonferrous metals, electronic information, electrical equipment, automotive, other).

In addition, the Study on the application framework and standardization demands of AI in intelligent manufacturing [153] highlighted the crucial role of AI in the future development of China's next generation intelligent manufacturing system with a rather limited number of existing AI standards for industrial implementation, thus leading to new standards to meet current demands for AI technology.

Despite the national focus of the standardization guidelines, orientation towards the smart factory concept and globally available technology applied in already defined architectural frameworks, it inevitably implements international norms in technical part (B). This particularly applies to the BA, BE, BF and partly BD sections dealing with the integration and interconnection of hardware and software systems, along with data management, virtualization, asset digitization and cloud solutions. From the perspective of the steel manufacturing industry (covered by Part C) and especially the SCADA system, they significantly affect the layers of assets, integration, communication and information layers in RAMI4.0.

Given that the function layer is case-specific, we can expect the IMSA reference architecture to be in line with international standards in the part related to the 4th generation SCADA systems, i.e. an implicit implementation can be considered for the above segments in Table 2, cautiously excluding those standards that primarily define structural elements, product and life cycle management that might be approached from different angles to comply with the Chinese industry landscape [91].

3) EMPIRICAL AND BEST-PRACTICE APPROACH

As a commercial and empirical model derived from the generalization of practical experience, IBM's I4.0 reference architecture is declared to be open, modular, plant-specific, and vendor-independent. These key features address the non-functional requirements of performance, scalability, maintainability, availability, security, volume, manageability, and usability [154]. However, standards-based, as one of the key features, is somewhat scarcely defined. IBM's lead-by-architecture approach toward consumerization in manufacturing [154] references to ISA-95 layers in achieving hybrid cloud-based production IT by leveraging on the mostly proprietary solutions, applied within a three-layer architecture that separates the edge layer located within

TABLE 2. International standards implemented by reference architectures.

Standard	Year	Ed.[b]	Description	IoT-ARM	IMSA	IIRA IICF	RAM I4.0	SME	I4.0 RA	URM-MM
IEC 62601	2015	2	Industrial networks - Wireless communication network and communication profiles - WIA-PA	I	X	I	X		X	
IEC 62541	2015[a]	1	OPC Unified Architecture	I	X	X	X	X	X	
ISO/IEC 2382	2015	1	Information technology — Vocabulary	I		X	X		I	I
IEC 62714	2015[a]	2	Engineering data exchange format for use in industrial automation systems engineering - Automation markup language			X			I	
IEC 62591	2016	2	Industrial networks - Wireless communication network and communication profiles - WirelessHART	I	X	I	X	X	X	
IEC 61511-1	2016	2	Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements		I		X		X	I
ISO/IEC 18384	2016[a]	1	Information technology—Reference Architecture for Service Oriented Architecture (SOA RA)	I		X				I
IEC 62657	2017[a]	1	Industrial communication networks - Wireless communication networks	I	I	I	X		I	
IEC-PAS-63088	2017	1	Smart Manufacturing – Reference Architecture Model Industry 4.0 (RAMI4.0)	I			O			I
IEC 62948	2017	1	Industrial networks - Wireless communication network and communication profiles - WIA-FA	I	X		X		X	
IEC 62351-9	2017	1	Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment				X		I	I
ISO 14306	2017	2	Industrial automation systems and integration — JT file format specification for 3D visualization					X	I	
ISO 1101	2017	4	Geometrical product specifications (GPS) — Geometrical tolerancing — Tolerances of form, orientation, location and run-out	I	X			X	I	
ISO 19941	2017	1	Information technology—Cloud computing—Interoperability and portability	I	I	X			I	I
ISO/IEC 30141	2018	1	Internet of Things (IoT) — Reference Architecture	O		I	X			I
IEC PAS 63178	2018	1	Smart manufacturing service platform - Service-oriented integration requirements of the manufacturing resource/capability	I			X			I
ISO 5458	2018	3	Geometrical product specifications (GPS) — Geometrical tolerancing — Pattern and combined geometrical specification	I	X			X	I	
IEC 21823	2019[a]	1	Internet of things (IoT) — Interoperability for IoT systems	I	I	I	X		I	I
IEC 61784-2	2019	4	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	I	X	I	X	X	X	
ASME Y14.41	2019	3	Digital Product Definition Data Practices	I				X		
ISO/TS 15926-4	2019	2	Industrial automation systems and integration — Integration of life-cycle data for process plants including oil and gas production facilities — Part 4: Initial reference data					X	I	
IEC 62832	2020[a]	1	Industrial-Process Measurement, Control And Automation - Digital Factory Framework	I			X		I	I
ISO/IEC 30161	2020	1	Internet of Things (IoT) — Requirements of IoT data exchange platform for various IoT services	I	I	I	X		I	I
IEC 62890	2020	1	Industrial-process measurement, control and automation - Life-cycle-management for systems and components				X		I	
ISO/ASTM 52915	2020	3	Specification for additive manufacturing file format (AMF)					X	I	
ISO 23952	2020	1	Automation systems and integration — Quality information framework (QIF) — An integrated model for manufacturing quality information					X	I	I
IEC 20924	2021	2	Internet of Things (IoT) - Vocabulary	I		I	X		I	I
IEC 62061	2021	2	Safety of machinery - Functional safety of safety-related control systems		I		X		X	I
ISO 16792	2021	3	Technical product documentation — Digital product definition data practices	I	I			X	I	I
IEC 63278	N/A[c]		Asset Administration Shell for industrial applications	I			O			I
IEC 63270	N/A[c]		Industrial automation equipment and systems - Predictive maintenance		X		X			I

O - new standard. I - implicit compliance. X - explicit compliance. [a] Earliest publishing year of oldest valid standard in the group. [b] Oldest currently valid edition within the group. [c] Under development (not available).

OT/IT convergence, from plant-level and enterprise-level IT solutions. Given the IT components used across layers, IBM's reference architecture overlaps with the other considered architectures (IIRA, IoT-ARM, RAMI4.0, SME) on a technological and technical level. This affects device management, communication, control flow, data flow and data model, integration, security and connectivity at all three layers, and therefore explicitly implements the appropriate standards accordingly. Considering the general approach of openness, partnership solutions, open source and the mission of adapting to customer needs, which implies the gradual transformation and integration of existing systems, international standards derived from the aforementioned initiatives and strategies can only be implicitly or partially implemented on a use-case level.

The IIC's mission is digital transformation across industries and accelerating IoT adoption by identifying best technology practices and delivering transformative business value [155], [156]. As such, IIRA and IICF, although developed on the ISO/IEC/IEEE 42010 concepts and models, implement multiple industry-specific standards [157]. These standards are not comparable to those reference architectures shown in Table 2 that are local standards-oriented (IMSA), rely on the concept of Loosely Defined Standards (IVRA, I4.0-RA), in-depth manufacturing oriented (RAMI4.0) or provide procedural guidance (URM-MM). In addition, IIC is an Object Management Group (OMG) program, and implements related standards (UML, BPMN, COBRA, UML, SYSML, DDS) accordingly [158]. In the process of alignment and interoperability between IIRA (IICF) and Platform I4.0, the core connectivity standards (OneM2M, DDS, Web Services and OPC UA) were emphasized [134]. In that respect, a parallel can be drawn with IoT-ARM [159] which addresses multiple fields of application (transportation/logistic, smart home, smart city, smart factory, retail, e-health, environment) through the definition of a domain model. However, IoT-ARM does not explicitly address the same international standards as IVRA, but is predominantly focused on OASIS [160], W3C [161], OMG [158] standards and modeling languages [162], whereas the ISO/OSI/IEEE standards listed in Table 2 are rather implicitly adopted on a use case basis, depending on the domain model, i.e. field of application, and are therefore marked respectively.

4) ECLASS – CLASSIFICATION STANDARD

As stated in [163]: *"Without a unified underlying ontology, no communication with universally recognized significance can take place, which undermines cross-domain functionality"*. Following this statement, and in order to make reference architectural models applicable for ICS development and deployment in real-world smart factories, standardization and harmonization of various reference models is an obvious necessity. Nonetheless, if a cross-industry classification system and a common language of electronic data exchange are not defined and globally accepted, interoperability and interconnectivity at the product and service level, as pillars of IoT networks, will be compromised. This is significant, not only for providing machine-interpretable data valid throughout the product life cycle, but also for the development, maintenance and future revampings of SCADA systems that rely on interoperable hardware and software components attainable in the global marketplace.

Founded in 2000, Eclass [164] provides standard descriptions of products and services, together with their functions and structural elements based on the ISO, IEC and ETIM compliant data model with data structures implementing IEC 61360, ISO 13584 and German national DIN 4002 standards, wheres belonging properties are restructured in accordance with DIN 4002. Although Eclass is predominantly oriented towards product classification and the related common data language, achieving a uniform application of relevant data across the development, manufacturing and sales phases, it is also machine-interpretable, and thus enables communication across devices and services in IoT networks using BMEcat, AutomationML, Administration shell and OPC UA data format ensuring sector-independent semantic interoperability at the asset level, scaling up to ERP, PLM, MES systems and further through the value chain enabling communication and cooperation of partners. Globally recognized, Eclass is already the de facto standard in B2B applications used by 3,500 companies worldwide. It currently provides 45,000 product classes with 19,000 belonging property descriptions with unique, machine-readable identifiers [165].

Eclass is not an architectural model and is therefore not included in Table 2. Nevertheless, in the context of I4.0, it brings a standardized product classification and a mechanism for the unhindered information flow that can be implemented across multiple reference architectural models as a prerequisite for data-driven smart manufacturing (IIRA, RAMI4.0, IoT/ARM), and the backbone of the connected factory concept (IVRA, IVRA/Next).

V. SCADA SYSTEM SECURITY

The security aspect of SCADA systems and ICS in a broader context is not the primary concern of this paper and it is not necessary for understanding the concept, architecture, design and other aspects of SCADA systems within I4.0 that have been discussed in previous sections.

However, it is necessary to keep in mind the importance of this topic in todays's ICS and SCADA systems, which are significantly more exposed to cyber threats by implementing I4.0 enabling technologies, and consequently, reaching a higher level of connectivity and integration that no longer keep OT out of the reach of IT network, such as this was the case with the first three generations of SCADA systems.

A. RESEARCH INTEREST

The importance of the security aspect in research is evident from the results of the database search. Applying the following search string:

("Abstract":"SCADA" OR "Abstract":"Supervisory control and data acquisition" OR "Abstract":"ICS" OR

"Abstract":"industrial control system" OR "Abstract": "distributed control system*") AND ("Abstract":"industrial automation" OR "Abstract":"industry 4.0" OR "Abstract": "IIoT" OR "Abstract":"industry" OR "Abstract": ""cyber?physical") AND ("Full Text.AND. Metadata":"process control" OR "Full Text.AND. Metadata":"manufacturing" OR "Full Text.AND. Metadata": "industrial process" OR "Full Text.AND. Metadata": "process control")*

in IEEE Xplore alone, resulted in 284 titles published in the last five years, which, when reduced to 124 titles based on the context relevance, still contained 41 titles, i.e. 33% with security as dominant topic, although there was no keyword *security* or *cybersecurity* in the search string.

The reason for such an emphasized presence of the research topic lies in the significant importance that ICS security has gained in the last decade due to the exponential growth in the number of cyber attacks, their increasing level of sophistication, and severe impact on industry and critical infrastructure.

Although cyber attacks on SCADA systems are not a new problem, the number of reported incidents began to increase dramatically after the year 2000, i.e. when SCADA systems able to communicate via TCP/IP protocol were introduced [167]. However, the security aspect of ICS and SCADA systems was not considered a global issue until the discovery of the Stuxnet worm, developed in 2010 with the specific purpose of targeting ICS [168], and two years later, the Shamoon virus responsible for the attack on Saudi Aramco, the world's largest oil company [169], [170]. In addition, the 2015 Black energy cyber attack on the Ukrainian power grid [171] exposed the weakness of critical infrastructure and raised questions about the security of other power grids around the world.

These and other attacks that followed, raised the level of awareness of the importance of ICS, SCADA and Cyber-physical systems security issues, and resulted in a growing interest of the scientific community in exploring the current state of cybersecurity and providing solutions to protect industrial facilities form cyber attacks.

As a result, multiple surveys, reviews and systematic literature overviews have been published, covering the domain of security within I4.0, CPS, ICS, SCADA systems and the manufacturing industry in general, providing insight into the security risks and implementation of digital security measures in these environments [167], taxonomy of attacks [172], [173] and security standards developed for SCADA networks [173], intrusion detection systems [57], general attack vectors and potential mitigation strategies [174], quantitative evaluation and comparison of vulnerabilities and potential impacts [175].

B. PRACTICAL SIGNIFICANCE

The better domain knowledge, which resulted from aforementioned research, provided a strong basis for building simulation environments that are proposed in form of various SCADA testbeds [57], [176], able to visualize the stages of a cyber attack [177], and a toolbox for attack simulation to train and test the security mechanisms [178].

These simulation environments and tools have provided methods for analyzing various types of threats such as stealthy attack [179], or new family attacks such as Heuristic Inference Attacks [180], related system vulnerabilities as well as exploring new ways to protect critical infrastructures such as Blockchain [181] and implementation of AI algorithms for intrusion detection systems (IDS) such as Support vector machine (SVM) access to Modbus TCP protocol [182].

Furthermore, numerous solutions have been proposed, enhancing SCADA security within various domain of implementation, such as cyber attacks on cloud SCADA systems [183], end-to-end encryption between SCADA and Open PLC [184], fuzzing SCADA protocols in smart grids [185], and cryptographic considerations addressing legacy structures using insecure communication protocols [186].

The bottom line is that with the increased level of interconnectivity and exposure to the internet, the overall exposure to threats is rising as well. As a consequence, attacks on ICS are inevitable. Accordingly, there are multiple security recommendations and guidelines from relevant institutions, such as the National Institute of Standards and Technology (NIST) [86] and the European Union Agency for Cybersecurity (ENISA) [188]. Considering the difference between standard IT system and ICS/SCADA system, Thames and Schaefer in Cybersecurity for Industry 4.0 [189] suggest following generic steps in forensic incident response model:

- Prepare: Understand ICS/SCADA system architecture, requirements, and related possible attacks.
- Detect: Determine type of attack and affected areas.
- Isolate: Isolate infected areas.
- Triage: Identify and prioritize data sources.
- Respond: Perform data analysis and acquisition.
- Report: Update system architecture, requirements, review findings and create reports.

When an incident occurs, it is essential to undertake a forensic response. However, the above steps can vary significantly depending on the architecture of the ICS/SCADA system, the implemented technology, the level of connectivity and convergence of OT/IT networks and IoT devices on the production floor. In this respect, the first step is crucial. Without knowledge the system architecture and the controlled industrial process, it will be difficult to determine the key threats and the appropriate defense mechanisms.

VI. OPEN ISSUES AND CHALLENGES

A. DIVERGENCE OF REFERENCE ARCHITECTURES AND ARCHITECTURAL STANDARDIZATION

In this paper we have considered significant I4.0 architectural models with regard to their presence in scientific literature, global recognition, relevance for the manufacturing industry and the 4th generation SCADA systems. But even in this

reduced set, the divergence of reference architectures and implemented standards is evident, arising from different starting points and applied approaches.

1) NARROWING THE FIELD OF IMPLEMENTATION

The German Industry 4.0 initiative leads in the attempt to reduce disparities between reference architectures through numerous international collaborations with aim of harmonizing reference architectures [114], [116], [134], [135].

As constructive as these architectural alignments are, they also bring to the surface the fundamental differences in some aspects that prevent higher degrees of convergence between the reference architectures. Apart from the starting viewpoints and approaches, these differences are partly the result of the application of different basic and industry-specific standards [4], [107] with the further intention of uniform implementation across industries.

In these circumstances, in parallel with the harmonization of architectures, additional efforts are needed to match the reference architectures with the desired industry and implementation domain with the corresponding classification of adopted industry-specific standards, and to define multiple use scenarios across industries as a guideline for the implementation of the available reference architectures.

Although this work has already been done to some extent with numerous case studies and pilot projects in the case of RAMI4.0, and also IBM-RA which is derived from use cases, these examples are intended to demonstrate a wide application of respective architecture models across the industries, rather than finding the best match for a given field within the industry. This approach is not wrong, but no matter how flexible a reference architecture may be, advocating *"one size fits all"* approach might slow down the process of adopting I4.0 concept in cases where the implementation of the chosen reference architecture model proves to be too complex, e.g. when current industrial landscape demands retrofitting of existing equipment [190].

2) REDEFINING THE SCADA SYSTEM

In addition to the already adopted standards that expand IT and IoT vocabulary (IEC 20924, ISO/IEC 2382) in accordance with the I4.0 concept and reference architectures, SCADA systems need to be redefined in this regard as well. This relates to the previously discussed common misconceptions, ambiguous definitions and overlapping functions as a consequence of extending traditional ICS with disruptive technologies. Without establishing a common ground and a clear understanding of today's SCADA system, its boundaries and the range of its functions distributed across its elements, it will be difficult to proceed with a smooth transition to the next phase in evolution of industrial automation control systems.

In this regard, there are multiple standards that affect SCADA systems, including all standards in Table 2. However, there is a lack of international standards focusing on SCADA systems in general. Inserted into the ISO standards advanced search engine,[1] the keyword "SCADA" found zero standards with the exception of International Classification for Standards document, whereas IEC webstore[2] offered 205 documents related to SCADA systems, the vast majority of which relate to power systems, energy management and electric utility, and neither of those refers to SCADA as a topic in focus. The need to address recent changes in evolving SCADA systems, structurally and functionally altered by I4.0 paradigm, was recognized by the ISA112 SCADA Systems standards committee established in 2016 to address the system design, implementation, operation, and maintenance of SCADA systems in a range of industries and to support the overall integrity and reliability of these systems [191].

Although the I4.0 paradigm offers a common ground for different industries, there is a big difference in application and architecture. For example, IoT networks across industries (transport, health, agriculture, utilities, energy, manufacturing) have significant differences in architecture, quality requirements and the type of devices included in the control systems. As a consequence, the SCADA system can be interpreted differently as well, and needs to be defined accordingly. These interpretations should not affect the standards, but need to be addressed within the reference architectures instead. Nevertheless, in addition to developing a series of ISA standards and technical reports, the purpose of ISA112 is to document best practices and industry-specific guidelines to complement the developed standards.

B. DEVELOPMENT AND TRANSITION OF SCADA SYSTEMS TOWARD I4.0

According to the conclusions of the workshop with European technology leaders on enabling technologies for Industry 5.0 held in 2020 [192], Industry 4.0 is still unfolding, i.e. its concept and associated technologies are still not broadly adopted, which, apart from small and medium-size companies, considerably affects traditional industries as well. SCADA systems are no exception to this trend, and particularly those that can be found in steel plants.

1) OBSOLETE TECHNOLOGY AND ARCHITECTURAL INCONSISTENCY RESULTING FROM GRADUAL UPGRADES

One obvious reason for dated SCADA systems is the operative lifetime of the equipment in such industrial facilities, which easily extends over twenty years. Although this cannot be the case for IT hardware, a common practice in replacing or upgrading IT hardware is to gradually migrate the existing SCADA software to the new one. This practice has numerous disadvantages, but it reduces the downtime needed for commissioning of the new SCADA system, which could otherwise take weeks and greatly impact the production plan. For the same reason, major revamping or replacement of the entire SCADA system is not considered unless there is an obvious and significant improvement in question. Another

[1] ISO search engine: https://www.iso.org/search.html?q=scada
[2] IEC webstore search: https://webstore.iec.ch/searchform&q=scada#

reason is related to the potential risk for stability in process control due to the human element, i.e. operators who need time to adjust to the new SCADA system after years of using the old one. As a consequence, it is more common to perform partial upgrades, i.e. improving the existing SCADA system with new functionalities or adding new software packages and equipment that operates independently or can be integrated into the existing system to some extent. When it comes to smart manufacturing, these targeted upgrades may involve IIoT devices on plant floor, process optimization, predictive maintenance, advanced data collection, real-time analytics and reporting, access to cloud services and various virtualization solutions and platforms. As previously shown in Fig. 5, these elements significantly influence traditional ICS and thus SCADA systems as well by creating the structure that no longer benefits from the separation of functional layers of the ISA-95 model, and also does not fit to any of the discussed architectural models. This sort of unconformity is additionally emphasized by integration and interconnection issues within such structures that are greatly influenced by proprietary protocols, monolithic applications and closed SCADA systems.

2) PROPRIETARY SCADA AND LEGACY SYSTEMS DRAWBACKS

A systematic approach is necessary to address the above issues of integration, interconnection and architectural inconsistency. Whereas the first two are covered by reference architecture models at the ICS level in the domain of horizontal and vertical integration across layers or levels (RAMI4.0, IIRA, IVRA-Next, IBM Industry 4.0 RA), and within the SoA concept encompassing IoT heterogeneous networks, SCADA systems are somewhat left behind. One of the reasons is because SCADA system development, when it comes to complex production processes, is normally in the hands of system integrators, and the production facility only uses the final product. Another reason is the complexity of SCADA system development tools, i.e. Integrated Development Environment (IDE) platforms which are traditionally developed by major industrial companies, such as General electrics, Siemens, Schneider Electric, Yokogawa, Honeywell, ABB, Rockwell automation, Mitsubishi electric and Emerson, which typically make up the top ten SCADA vendors on industry-related reports and websites [193], [194], [195]. Considering the SCADA market size valued at USD 35.38 billion in 2021 and expected to reach USD 61.22 billion by 2030 [196], with continuous growth rate of 6.64% in the period 2017–2021 [197] and IIoT market expected value of USD 276.79 billion by 2029 [198], neither vendors nor system integrators have an interest in reducing the SCADA market divergence, product differentiation, or directing SCADA systems towards open source solutions.

Proprietary SCADA systems in themselves are not necessarily an obstacle to advance toward higher levels of integration and interconnectivity, which are the objectives embedded into each reference architecture considered. Ignition industrial application platform [199] is a good example in this regard, with server-centric web-deployment, modular configurability, cross-platform compatibility, embracing IIoT, open standards and seamless connectivity. However, decades of SCADA systems IDEs continuous development and evolution in a closed circle of global companies manifests the following: 1) Vendors offering industrial hardware and software as complete solutions in the field of industrial automation expectedly favor the integration of their own products, e.g. Totally Integrated Automation Portal [200] which integrates multiple basic development software achieving integrated engineering and development of multiple products and solutions. Whereas this is a good approach for reducing development time, minimizing bugs in software, raising the level of security and unifying the development platform, it is a closed system. Although integrated platforms of this type additionally support open network protocols, cross-network data exchange and cloud solutions, the level of integration within a defined SCADA network is significantly limited; 2) As previously mentioned, the service lifetime of industrial equipment spans over decades. For this purpose, industrial control systems are built with longevity in mind. As their integral part, SCADA systems are forced to follow the same approach which faces significant challenges. In order to ensure backward compatibility with previous versions over such a long period of time, it is very difficult to perform a clean slate in adopting new technologies, while simultaneously ensuring compatibility with stand-alone monolithic desktop applications. This is particularly emphasized nowadays, in the era of I4.0 and emerging IIoT. Global companies are able to provide integrated and robust solutions that have significant value in the industrial environment, but these systems, burdened with obsolete technology, have difficulty to progress toward web and IoT technologies as a comprehensive solution, i.e. development environment and SCADA product.

3) SCADA DEVELOPMENT, DEPLOYMENT AND VENDOR SUPPORT

SCADA systems differ across the industries. These differences are related to size, architecture, complexity, level of integration and interoperability, etc., and significantly affect the development process in terms of complexity and time. In the case of steel plants, as the one depicted in Fig. 2, the total time from the planning of the entire project to the plant in production takes years. Fig. 7 shows the basic concerns and activities affecting the SCADA system development across the life cycle phases of such a production facility, that emphasizes the dependencies of respective concerns in relation to others within the same time frame. These dependencies are marked as *indirect*, when there is no immediate mapping to SCADA system development process, i.e. intermediate activities are implied, or *direct* in case the modification of the SCADA system is an immediate consequence of changes in the given elements.

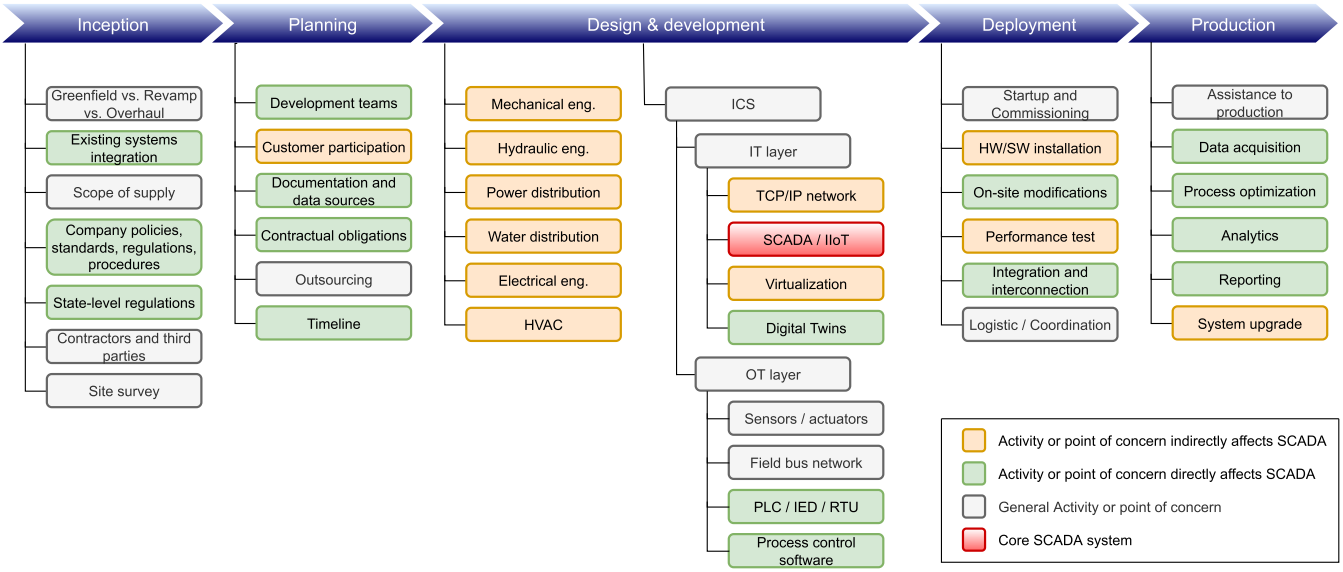


FIGURE 7. SCADA development considerations within the broader context of production plant development life cycle.

Placing the development of SCADA in this broader context is significant for understanding the importance of the time component in the overall process. Although SCADA development begins at later stages, its key elements are defined in a contract signed prior to any development activity. This initial phase alone can take months through extensive negotiations in the sales process, especially if the client is a state or state-owned company.

Depending on the size and complexity of the plant facility, additional technical and logistic data gathering through plant survey is required. The success of this phase greatly influences the rest of the process as its purpose is to establish actual field conditions, align contract details with site conditions, and gain direct contact with the client's technical personnel who can be of great assistance in later stages. Once the necessary data is obtained, the planning phase is approached according to the defined scope of supply and agreed deadlines. Depending on the availability and engagement of adequate experts, forming teams in this phase is challenging. These two phases extend through several months.

The design and development phase encompasses design and construction of heavy machinery, medium voltage distribution, electrical, hydraulics, water and heating, ventilation and air conditioning (HVAC) projects. ICS development may overlap with these activities in the OT segment and network projects, but SCADA system development depends on a wide range of data and documentation generated by all previous development segments and process control software, as shown in Fig. 7. Therefore, even if it overlaps with other activities, the SCADA system develops last. The timeline for the overall phase of design and development may vary significantly depending on the scope of the project. In the case of greenfield projects, there will be significantly more work in the domain of hardware design and development, whereas revamping projects will greatly reduce this part, but will emphasize the SCADA segment in the integration and adaptation of existing equipment and solutions. All taken in consideration, a time frame of two to three years can be considered realistic for this phase.

The duration of the start-up and commissioning phase largely depends on how well prepared and executed all previous phases are. In addition, it reflects the flexibility of the contracting parties in case of any deviations between the agreed and the delivered. Realistically, minor modifications to the system are expected prior to and after cold and hot tests, and even later, in assistance to production. The overall expected duration is six to twelve months, although various types of delays are expected in this phase as well.

Considering the external aspects of steel manufacturing plants construction, such as financial, geostrategic and political, global steel demand and price fluctuations, regional conflicts and crises, there are also a number of external influences as well that can significantly extend the duration of development.

In conclusion, the time frame for an entire project of this size is difficult to estimate. However, even a roughly estimated time duration across the project life cycle phases results in a total duration of at least four to five years, and reveals the problem of the prematurely obsolete SCADA system entering production. Taking into account the equipment and the overall ICS lifetime, the SCADA system is expected to be modified and upgraded multiple times over the years, and vendor support is essential to the expected compliance issues when dealing with OS upgrades, connectivity and third party software packages integration, and even SCADA components.

However, the support life cycle for SCADA components from major vendors is limited to five years from release

date [201], [202], [203]. Under these circumstances, customers are forced to upgrade the SCADA system, as well as licenses, immediately after the plant start-up and to continue to do so in five-year cycles. While licensing represents only unwanted additional expenses, each of a SCADA project containing customized constructs, such as custom-developed code or ActiveX controls, may result with functionality problems for individual elements or even extend to other SCADA components. Following standard safety procedures, any activity of this type must be tested which requires production stoppage causing additional costs. In consequence, this is one of the practical reasons that slows down transition of existing SCADA systems toward the I4.0 concept.

This may not affect all life cycles of all SCADA systems equally. Minor and partial projects can be developed within a few months. However, these projects are modifications or additions to existing larger SCADA systems that already manifest the issue in question, and in case of any incompatibility with existing SCADA systems, they are most likely to face the same lack of support due to end of life cycle.

VII. FUTURE DIRECTIONS BEYOND I4.0

The concept of Industry 4.0 is still not widely accepted, but innovation shows no signs of deceleration. It pushes the boundaries even further and continues to change the landscape of the industry. However, driven by emerging technologies, focused on the efficiency and flexibility of production, and geared towards short-term economic value, technological progress in the industry so far does not make sense without wider significance for society, i.e. future directions beyond I4.0 needs to align with our priorities as a society.

A. SOCIETY 5.0 AND INDUSTRY 5.0

The I4.0 paradigm shift, which extends to wider social significance, was first addressed by the Japanese government in 2016, in the document The 5th Science and Technology Basic Plan [204], under the initiative ''Society 5.0'' [6] Where the Society 5.0 is defined as *"A human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspace and physical space"*. Thus defined, it implies a high degree of convergence between the virtual and physical worlds, consequently leveraging on ubiquitous pervasive technology.

Consistent with the idea of broader societal impact, several concepts and plans have been adopted under the umbrella of Japan's New Industrial Revolution (NIR) that address implications for inclusive and sustainable industrial development [89], leading to Connected industries [205] as the fundamental concept supporting Society 5.0.

Narrowing it down to the industrial domain, the more common term is ''Industry 5.0'' (I5.0) and it is directly or indirectly addressed by numerous initiatives aimed at industry and technology advancement projections for this decade [192], [206], [207].

Although it is the next number in the sequence, I5.0 is not a chronological continuation of the I4.0 paradigm, nor its alternative. I5.0 rather complements and extends existing concepts beyond a purely techno-economic vision by adding environmental and social dimensions as decisive factors for the integration of industry into the future society [208]. In the simplest terms, I5.0 makes I4.0 more complete, human-oriented, resilient and sustainable in the long term, thus becoming a provider of prosperity for society, i.e. stakeholders instead of shareholders. To achieve this, I5.0 leverages continuous and rapid advancement of technology. Analysis and identification of current research trends in domain of I5.0 [209] singled out AI, Big data, supply chain, digital transformation, ML and IoT as key enablers identified by researchers. The Implementation of these technologies elevate the level of broadly applied automation to multiple domains of human activity, building an ecosystem that will extend sustainability to other domains, such as environmental, social and political [210].

Orientation to new values has not been initiated by design. Instead, it is a result of the implementation and maturing process of I4.0. Regardless of the relatively short period of existence, i4.0 has revealed three negative aspects of its primary orientation toward short-term economic value: 1) A worker is considered a cost within his/her limitation to continually adapt to evolving technology. With such a view of the worker, it is logical to try to replace him with appropriate technology, i.e. to exclude humans from the process where possible; 2) The primary focus on increasing cost efficiency and maximizing profit does not reflect well on long-term sustainability, i.e. respecting planetary boundaries and the global consensus on reducing greenhouse gas emissions, waste and environmental impact; 3) Globalized production without resilient strategic value chains and failure do include sustainability in industrial processes that addresses the energy consumption and alternative resources, have led to the system becoming vulnerable to regional geopolitical shifts and crises such as Brexit, energy crisis due to the war in Ukraine and sanctions against Russia, or the previous Covid-19 pandemic, the last two of which highlighted the fragility of energy-intensive manufacturing industries.

B. SHIFT IN WORKFORCE DUE TO CHANGES IN SOCIETY

Whereas aspects of sustainability and resilience, however complex, can be addressed through the adoption and implementation of appropriate strategies that are subject to planning and for which specific time frames can be set, the firstly addressed aspect involving insufficient and/or inadequate manpower, partly the result of a decade-long implementation of a human-exclusive concept, is a significantly more complex problem to solve. In addition, the workforce that currently constitutes the majority relies significantly on millennials who are conceptually not the same as the previous generation of workers. Recent research finds millennials differ from previous generations in ideas, expectations, perceptions, behaviors and engagement [211], [212]. They are not driven by common objectives unless aligned with their personal goals, but are attracted to challenging tasks,

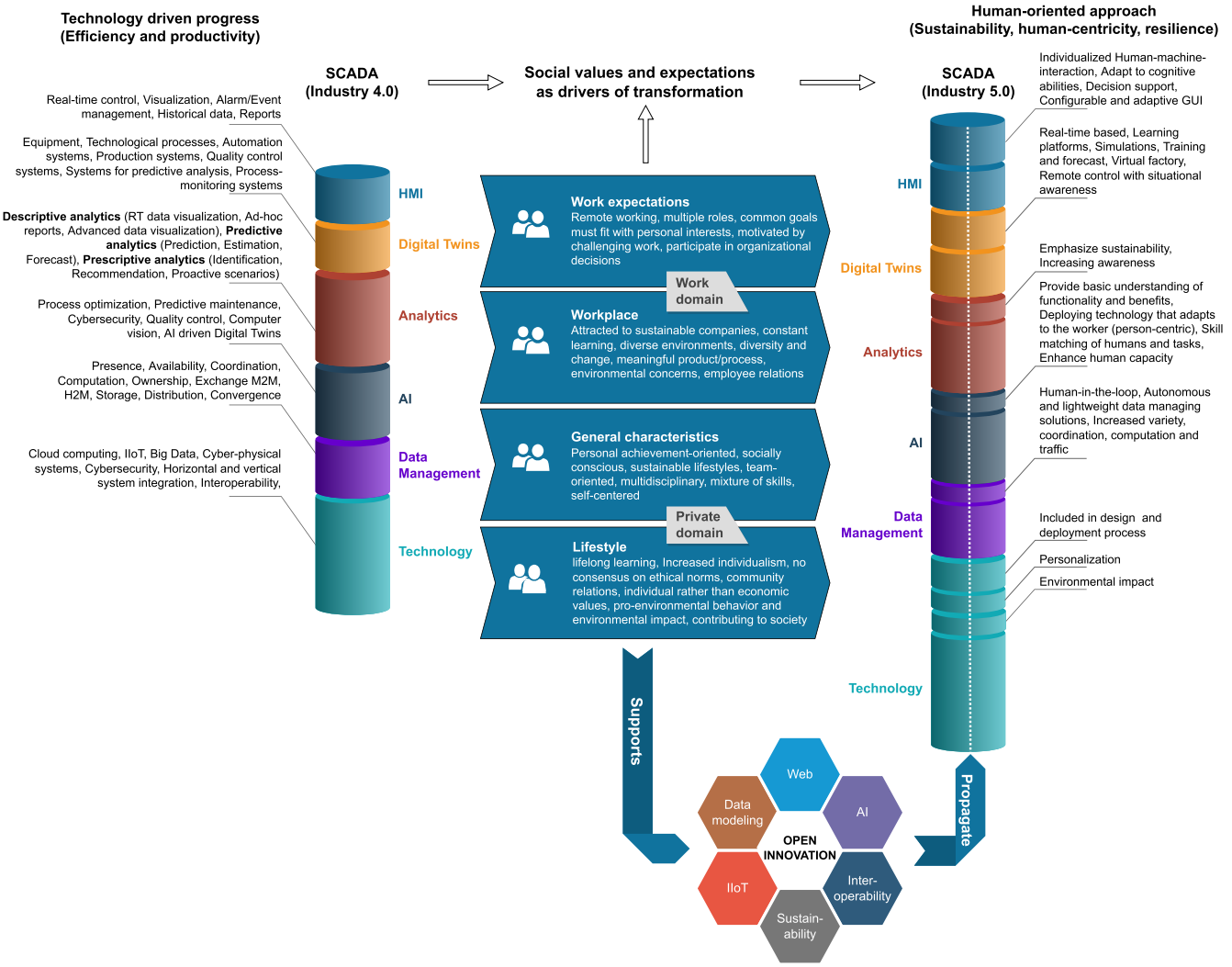


FIGURE 8. SCADA transition toward Industry 5.0 influenced by social values.

lifelong learning, a diverse and dynamic working environment, and self-achievement. In general, millennials can be considered as their own achievement oriented individuals and team-oriented at the same time, with an attitude of diversity and desire to participate in organizational and strategic decisions [7]. More broadly, millennials have strong attitudes toward community and employee relations, service and product quality, global governance, diversity, individual values, and share a common concern for sustainability [213].

Viewed in a broader social context, these characteristics, attitudes, perceptions, habits and behavior, impacts employment and working environment, and consequently the approach of employers as well. Survey of experiments discussing the younger generation as a driving force toward achieving the sustainable development goals [214] has portrayed millennials as socially conscious with pro-environmental behavior and work value, preferring sustainable lifestyles and sustainable consumption, and concluded that millennials are attracted to sustainable companies. Furthermore, in the context of Sustainable Development Goals (SDGs), the study has shown that people are willing to accept lower salaries in order to be employed by a company that is more focused on the SDGs.

These findings are a good indicator for companies to review their employment policies and accept changes in society in order to remain competitive in the employment market. Taking into account the aforementioned social preferences and characteristics, this will be particularly challenging for the manufacturing industry, which is energy-intensive and the furthest from achieving the SDGs.

C. IMPACT OF HUMAN-CENTRIC APPROACH TO SCADA SYSTEM

Addressing the transition towards a sustainable, human-centric and resilient European industry, as well as its technological frameworks [192], [208], six categories have been identified as enabling technologies: 1) Individualized human-machine-interaction; 2) Bio-inspired technologies and smart materials; 3) Digital twins and simulation; 4) Data transmission, storage, and analysis; 5) Artificial Intelligence;

6) Technologies for energy efficiency, renewables, storage and autonomy;

With the exception of Bio-inspired technologies, they all have an impact on ICS, whereas individualized human-machine interaction, digital twins and AI directly affect the functionality, structure and life cycle of SCADA systems.

Addressing the human-centric approach as one of the three key motives for the transition to I5.0, Fig. 8 depicts the transition of the SCADA system from I4.0 to I5.0 driven by the aforementioned changes in society, i.e. social values and the expectations of the the new generation of workforce.

Broken down into its basic segments, which are directly affected by the human-centric approach in the transition to I5.0 (Technology, Data Management, AI, Analytics, Digital Twins, HMI), the SCADA system aligned with the I4.0 concept is functionally oriented towards efficiency and productivity implementing corresponding solutions associated with each segment respectively, as shown in the figure.

Taking into account societal values and expectations in given categories (Work Expectations, Workplace, General Characteristics, Lifestyle), the I5.0 compliant SCADA system shown on the right has undergone changes resulting in more inclusive people and personalized technology, with workers involved in the design and implementation process, data management and an increased level of understanding of implemented AI solutions and analytics. Furthermore, digital twins extend to real-time learning platforms and simulations that can model entire systems (virtual factory) evolved to meet changing worker skills, training requirements and raised levels of operational safety. HMI, which uses AI, becomes significantly more individualized by adapting to the cognitive abilities of the operator by providing a customizable GUI and real-time decision support systems.

Such an inclusive SCADA system, and the industry in general, can further benefit from a participatory society that has a strong attitude towards community and knowledge sharing. These are the principles that underpin open innovation which has already proven to be beneficial in numerous fields including the manufacturing industry [215], and can bring new values that can be propagated throughout the entire system.

VIII. LIMITATIONS

In this paper, we provided a comprehensive view on the SCADA systems within the I4.0 paradigm and the smart factory concept with a focus on implementation in the continuous production process control within the steel industry domain. As important this is for the practical aspect, i.e. deeper insight and better comprehension of dedicated SCADA systems in the domain of design, development, deployment and overall adaptation to industry-specific conditions and requirements, as a consequence of narrowing the field of implementation with simultaneous goal to encompass a broader context so that is clearly understood, following limitations stands out: 1) Detailed assessment of industrial and IoT protocols, and networks. Although some protocols are addressed in Sect. IV, covering reference architectures, there is more to address on this subject which is significant for overall ICS quality requirements, i.e. availability and reliability. 2) Digital twins in SCADA systems, their role and significance for overall smart manufacturing. Sect. VI introduces digital twins as part of SCADA transition toward I5.0, i.e SCADA segment responsible for real-time based learning platforms, simulations, virtual factory, training and forecast. However, these roles and concepts are not further elaborated, as well as the concept of digital twins itself. 3) Analysis of the existing SCADA systems on the market and comparison between proprietary and free open-source solutions, relevant to discussion in Sect. V, has not been performed.

Although all of the above points are significantly relevant to the matter in hand, considering the depth of the field, each represents a separate topic, and thus exceeds the limits of this work. In addition, this paper has only partially addressed I4.0 enablers, leaving out enabling technologies and assets that includes robotics and collaborative robots (cbots) in particular, as well as smart products, 3D printing, bio-inspired technologies and smart materials. As relevant as these enablers are for the overall concept of I4.0 and manufacturing industry in general, they have been omitted on account of their relevance to the discussed specific field of implementation. However, this does not mean that some of them are not relevant in a more detailed discussion of future trends and advancement of process control systems within the I5.0 paradigm.

REFERENCES

[1] M. S. Knudsen, J. Kaivo-Oja, and T. Lauraeus, "Enabling technologies of industry 4.0 and their global forerunners: An empirical study of the web of science database," *Commun. Comput. Inf. Sci.*, vol. 1027, pp. 3–13, Jun. 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-21451-7_1

[2] T. Yang, X. Yi, S. Lu, K. H. Johansson, and T. Chai, "Intelligent manufacturing for the process industry driven by industrial artificial intelligence," *Engineering*, vol. 7, no. 9, pp. 1224–1230, Sep. 2021, doi: 10.1016/j.eng.2021.04.023.

[3] S. Vaidya, P. Ambad, and S. Bhosle, "Industry 4.0—A glimpse," *Proc. Manuf.*, vol. 20, pp. 233–238, Jan. 2018, doi: 10.1016/J.PROMFG.2018.02.034.

[4] Y. Lu, S. P. Frechette, and K. C. Morris, "Current standards landscape for smart manufacturing systems," in *Proc. NISTIR*, vol. 8107, Feb. 2016, pp. 1–39, doi: 10.6028/NIST.IR.8107.

[5] A. Sigov, L. Ratkin, L. A. Ivanov, and L. D. Xu, "Emerging enabling technologies for industry 4.0 and beyond," *Inf. Syst. Frontiers*, pp. 1–11, Jan. 2022. [Online]. Available: https://link.springer.com/article/10.1007/s10796-021-10213-w#citeas, doi: 10.1007/s10796-021-10213-w.

[6] Council of Science, Cabinet Office, and Government of Japan. *Society 5.0*. Accessed: Apr. 9, 2022. [Online]. Available: http://press-pubs.uchicago.edu/founders/

[7] K. L. Zabel, B. B. J. Biermeier-Hanson, B. B. Baltes, B. J. Early, and A. Shepard, "Generational differences in work ethic: Fact or fiction?" *J. Bus. Psychol.*, vol. 32, no. 3, pp. 301–315, Oct. 2016, doi: 10.1007/s10869-016-9466-5.

[8] P. Adolphs and U. Epple, "Status report reference architecture model industrie 4.0 (RAMI4.0)," Assoc. Elect., Electron. Inf. Technol. (VDE), German Elect. Electron. Manuf. Assoc. (ZVEI), Düsseldorf, Germany, Jul. 2015. [Online]. Available: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report__Reference_Archtitecture_Model_Industrie_4.0__RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf

[9] Energy Solution Center. *Electric Arc Furnace Energy Consumption*. Accessed: Mar. 28, 2022. [Online] Available: http://heattreatconsortium.com/metals-advisor/electric-arc-furnace/electric-arc-furnace-energy-consumption/

[10] O. Lozynskyy, A. Lozynskyy, Y. Paranchuk, R. Paranchuk, Y. Marushchak, and A. Malyar, "Analysis and synthesis of intelligent system for electric mode control in electric arc furnace," in *Analysis and Simulation of Electrical and Computer Systems* (Lecture Notes in Electrical Engineering), vol. 452. Cham, Switzerland: Springer, 2018, pp. 111–130. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-63949-9_7, doi: 10.1007/978-3-319-63949-9_7.

[11] D. Zhai. (Jul. 2021). *Characteristics of Intelligent Electric Power Supply System for Electric Arc Furnace*. Accessed: Mar. 10, 2022. [Online] Available: https://www.linkedin.com/pulse/characteristics-intelligent-electricpower-supply-arc-daisy?trk=public

[12] Tenova S.P.A. *Technology Solutions in Metals and the Mining Industries*. Accessed: May 14, 2022. [Online]. Available: https://tenova.com/technologies

[13] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," in *Proc. IEEE Int. Conf. Autom. Sci. Eng.*, Oct. 2018, vol. 34, no. 8, pp. 89–113, doi: 10.1007/978-3-319-75880-0_5.

[14] D. Reguera-Bakhache, I. Garitano, R. Uribeetxeberria, C. Cernuda, and U. Zurutuza, "Data-driven industrial human-machine interface temporal adaptation for process optimization," in *Proc. 25th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2020, pp. 518–525, doi: 10.1109/etfa46521.2020.9211930.

[15] S. Hourlier, "For our complex future, don't give us AI, give us intelligent assistance (IA): The case for avionics," in *Advances in Artificial Intelligence, Software and Systems Engineering* (Advances in Intelligent Systems and Computing), vol. 1213. Cham, Switzerland: Springer, Jul. 2021, pp. 16–21, doi: 10.1007/978-3-030-51328-3_3.

[16] World Steel Association AISBL, Worldsteel News. *Sustainability Indicators*. Accessed: Apr. 17, 2022. [Online]. Available: https://worldsteel.org/steelby-topic/sustainability/

[17] N. Gross and A. Kluge, "Predictors of knowledge-sharing behavior for teams in extreme environments: An example from the steel industry," *J. Cognit. Eng. Decis. Making*, vol. 8, no. 4, pp. 352–373, Jul. 2014, doi: 10.1177/1555343414540656.

[18] A. Banerjee, A. R. M. Forkan, D. Georgakopoulos, J. K. Milovac, and P. P. Jayaraman, "An IIoT machine model for achieving consistency in product quality in manufacturing plants," 2021, *arXiv:2109.12964*.

[19] F. Li, A. Yang, H. Chen, G. Sun, F. Wang, Y. Xie, J. Li, and J. Shen, "Towards industrial Internet of Things in steel manufacturing: A multiple-factor-based detection system of longitudinal surface cracks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 4627–4635, doi: 10.1109/bigdata50022.2020.9378300.

[20] S. Jaloudi, "Communication protocols of an industrial Internet of Things environment: A comparative study," *Future Internet*, vol. 11, no. 3, p. 66, Mar. 2019, doi: 10.3390/fi11030066.

[21] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti, "Design patterns for the industrial Internet of Things," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Jun. 2018, pp. 1–10. [Online]. Available: https://ieeexplore.ieee.org/document/8402353

[22] E. Tomur, U. Gulen, E. U. Soykan, M. A. Ersoy, F. Karakoc, L. Karacay, and P. Comak, "SoK: Investigation of security and functional safety in industrial IoT," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2021, pp. 226–233, doi: 10.1109/csr51186.2021.9527921.

[23] S. G. Abbas, F. Hashmat, and G. A. Shah, "A multi-layer industrial-IoT attack taxonomy: Layers, dimensions, techniques and application," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1820–1825, doi: 10.1109/trustcom50675.2020.00249.

[24] D. L. Tran, T. Yu, and M. Riedl, "Integration of IIoT communication protocols in distributed control applications," in *Proc. IECON 46th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2020, pp. 2201–2206, doi: 10.1109/iecon43393.2020.9254220.

[25] M. Kostoláni, J. Murín, and S. Kozák, "An effective industrial control approach," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, 2019, pp. 911–914. [Online]. Available: https://ieeexplore.ieee.org/document/8859836

[26] H. Zhang and L. Wang, "Design of data acquisition platform for industrial Internet of Things," in *Proc. IEEE 3rd Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE)*, Sep. 2020, pp. 613–618, doi: 10.1109/iciscae51034.2020.9236827.

[27] H. Koziolek, A. Burger, M. Platenius-Mohr, J. Rückert, and G. Stomberg, "OpenPnP: A plug-and-produce architecture for the industrial Internet of Things," in *Proc. IEEE/ACM 41st Int. Conf. Softw. Eng., Softw. Eng. Pract. (ICSE-SEIP)*, May 2019, pp. 131–140, doi: 10.1109/ICSE-SEIP.2019.00022.

[28] 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. 78238–78259, 2018, doi: 10.1109/ACCESS.2018.2884906.

[29] G. Wang, M. Nixon, and M. Boudreaux, "Toward cloud-assisted industrial IoT platform for large-scale continuous condition monitoring," *Proc. IEEE*, vol. 107, no. 6, pp. 1193–1205, Jun. 2019, doi: 10.1109/jproc.2019.2914021.

[30] M. Salhaoui, A. G. Gonzalez, M. Arioua, J. C. M. Molina, F. J. Ortiz, and A. E. Oualkadi, "Edge-cloud architectures using UAVs dedicated to industrial IoT monitoring and control applications," in *Proc. Int. Symp. Adv. Electr. Commun. Technol. (ISAECT)*, Nov. 2020, pp. 1–6, doi: 10.1109/isaect50560.2020.9523700.

[31] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying fog computing in industrial Internet of Things and industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4674–4682, Oct. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8410462

[32] A. Chehri and G. Jeon, "The industrial Internet of Things: Examining how the IIoT will improve the predictive maintenance," in *Innovation in Medicine and Healthcare Systems, and Multimedia*, (Smart Innovation, Systems and Technologies), vol. 145. Singapore: Springer, 2019, pp. 517–527, doi: 10.1007/978-981-13-8566-7_47.

[33] H. Liu, Q. Li, G. Li, and R. Ding, "Life cycle assessment of environmental impact of steelmaking process," *Complexity*, vol. 2020, pp. 1–9, Dec. 2020, doi: 10.1155/2020/8863941.

[34] Bearing News. (Oct. 2020). *Inside the Steel Industry: How Bearings Survive Under Very Harsh Conditions*. [Online]. Available: https://www.bearing-news.com/inside-the-steel-industry-how-bearings-survive-under-very-harsh-conditions/

[35] R. Singh, "Production of steel," in *Applied Welding Engineering*, 3rd ed. Amsterdam, The Netherlands: Elsevier, 2020, pp. 35–52, doi: 10.1016/b978-0-12-821348-3.00006-9.

[36] M. Justus, K. W. Leege, P. Michel, A. Schamlott, and R. Steinbrück, "Improvements of the ELBE control system infrastructure and SCADA environment," in *Proc. Int. Conf. Accel. Large Experim. Control Syst. (ICALEPCS)*, Barcelona, Spain, Oct. 2017, doi: 10.18429/JACoW-ICALEPCS2017-THPHA027.

[37] M. D. Stojanović, S. V. B. Rakas, and J. D. Marković-Petrović, "Scada systems in the cloud and fog environments: Migration scenarios and security issues," *Facta Universitatis Electron. Energetics*, vol. 32, no. 3, pp. 345–358, 2019, doi: 10.2298/fuee1903345s.

[38] A. Y. Zomaya and S. Sakr, "SCADA systems in the cloud," in *Handbook of Big Data Technologies*, Cham, Switzerland: Springer, 2017, pp. 691–718. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-49340-4_20

[39] H. Tan, Z. Huang, and M. Wu, "An interactive real-time SCADA platform with customizable virtual instruments for cloud control systems," *J. Dyn. Syst., Meas., Control*, vol. 141, no. 4, Apr. 2019, doi: 10.1115/1.4041977.

[40] P. J. Chong. *How to Prevent Electromagnetic Interference From Ruining Your Devices*. Accessed: Apr. 25, 2022. [Online]. Available: https://blog.ttelectronics.com/electromagnetic-interference

[41] R. Dionísio, T. Lolić, and P. Torres, "Electromagnetic interference analysis of industrial IoT networks: From legacy systems to 5G," in *Proc. IEEE Microw. theory Techn. Wireless Commun. (MTTW)*, Oct. 2020, pp. 41–46. [Online]. Available: https://ieeexplore.ieee.org/document/9245057

[42] J. Wu, Y. Qi, G. Gong, J. Fan, M. Miao, W. Yu, J. Ma, and J. L. Drewniak, "Review of the EMC aspects of Internet of Things," *IEEE Trans. Electromagn. Compat.*, vol. 62, no. 6, pp. 2604–2612, Dec. 2020, doi: 10.1109/temc.2019.2957423.

[43] B. Chen, Y. Liu, C. Zhang, and Z. Wang, "Time series data for equipment reliability analysis with deep learning," *IEEE Access*, vol. 8, pp. 105484–105493, 2020, doi: 10.1109/access.2020.3000006.

[44] C.-Y. Lin, Y.-M. Hsieh, F.-T. Cheng, H.-C. Huang, and M. Adnan, "Time series prediction algorithm for intelligent predictive maintenance," *IEEE Robot. Autom. Lett.*, vol. 4, no. 3, pp. 2807–2814, Jul. 2019, doi: 10.1109/LRA.2019.2918684.

[45] J. Zenisek, J. Wolfartsberger, C. Sievi, and M. Affenzeller, "Streaming synthetic time series for simulated condition monitoring," *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 643–648, 2018, doi: 10.1016/j.ifacol.2018.08.391.

[46] E. Lughofer, R. Pollak, A.-C. Zavoianu, P. Meyer-Heye, H. Zorrer, C. Eitzinger, J. Lehner, T. Radauer, and M. Pratama, "Evolving time-series based prediction models for quality criteria in a multi-stage production process," in *Proc. IEEE Conf. Evolving Adapt. Intell. Syst. (EAIS)*, May 2018, pp. 1–10, doi: 10.1109/EAIS.2018.8397186.

[47] M. Eifler, F. Ströer, S. Rief, and J. Seewig, "Model selection and quality estimation of time series models for artificial technical surface generation," *Technologies*, vol. 6, no. 1, p. 3, Dec. 2017, doi: 10.3390/technologies6010003.

[48] Automation IT. *Data Aggregation Using Historians for Informed Decision Making*. Accessed: Mar. 15, 2022. [Online]. Available: https://www.automationit.com/blog/90-data-aggregation-using-historians-for-informed-decision-making

[49] A. Ioana and A. Korodi, "DDS and OPC UA protocol coexistence solution in real-time and industry 4.0 context using non-ideal infrastructure," *Sensors*, vol. 21, no. 22, p. 7760, Nov. 2021, doi: 10.3390/s21227760.

[50] S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "A survey of IIoI protocols," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–53, Apr. 2020, doi: 10.1145/3381038.

[51] I. Hedi, I. Špeh, and A. Šarabok, "IoT network protocols comparison for the purpose of IoT constrained networks," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, Jul. 2017, pp. 501–505, doi: 10.23919/MIPRO.2017.7973477.

[52] M. Iglesias-Urkia, A. Orive, M. Barcelo, A. Moran, J. Bilbao, and A. Urbieta, "Towards a lightweight protocol for Industry 4.0: An implementation based benchmark," in *Proc. IEEE Int. Workshop Electron., Control, Meas., Signals Appl. Mechtron. (ECMSM)*, May 2017, pp. 1–6, doi: 10.1109/ECMSM.2017.7945894.

[53] M. Stusek, K. Zeman, P. Masek, J. Sedova, and J. Hosek, "IoT protocols for low-power massive IoT: A communication perspective," in *Proc. 11th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Oct. 2019, pp. 1–7. [Online]. Available: https://ieeexplore.ieee.org/document/8970868

[54] I. Hubschmann. (Feb. 2021). *A Comparison of IoT Protocols for Developers*. Accessed: Apr. 11, 2022. [Online] Available: https://www.nabto.com/iot-protocols-comparison/

[55] A. J. Shenhar and B. Sauser, "Systems engineering management: The multidisciplinary discipline," in *Handbook of Systems Engineering and Management*, 2nd ed. Hoboken, NJ, USA: Wiley, 2009, pp. 117–154.

[56] Q. Li, Q. Tang, I. Chan, H. Wei, Y. Pu, H. Jiang, J. Li, and J. Zhou, "Smart manufacturing standardization: Architectures, reference models and standards framework," *Comput. Ind.*, vol. 101, pp. 91–106, Oct. 2018, doi: 10.1016/j.compind.2018.06.005.

[57] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *Int. J. Crit. Infrastruct. Protection*, vol. 34, Sep. 2021, Art. no. 100433, doi: 10.1016/j.ijcip.2021.100433.

[58] International Society of Automation (ISA). *ISA95, Enterprise-Control System Integration*. Accessed: Apr. 10, 2022. [Online] Available: https://www.isa.org/standardsand-publications/isa-standards/isa-standards-committees/isa95

[59] Y. Lu, K. C. Morris, and S. Frechette, "Standards landscape and directions for smart manufacturing systems," in *Proc. IEEE Int. Conf. Autom. Sci. Eng. (CASE)*, Aug. 2015, pp. 998–1005, doi: 10.1109/coase.2015.7294229.

[60] Trend Micro. *Industrial Control System*. Accessed: Apr. 11, 2022. [Online] Available: https://www.trendmicro.com/vinfo/us/security/definition/industrialcontrol-system

[61] M. Akerman, "Implementing shop floor IT for industry 4.0," Ph.D. dissertation, Dept. Ind. Mater. Sci., Chalmers Univ. Technol., Gothenburg, Sweden, Jul. 2018.

[62] M. H. Alquwatli, M. H. Habaebi, and S. Khan, "Review of SCADA systems and IoT honeypots," in *Proc. IEEE 6th Int. Conf. Eng. Technol. Appl. Sci. (ICETAS)*, Dec. 2019, pp. 1–6, doi: 10.1109/icetas48360.2019.9117330.

[63] M. Al-Fadhli and A. Zaher, "A smart SCADA system for oil refineries," in *Proc. Int. Conf. Comput. Sci. Eng. (ICCSE)*, Mar. 2018, pp. 1–6, doi: 10.1109/iccse1.2018.8373996.

[64] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018, doi: 10.1016/J.COMPIND.2018.04.015.

[65] H. Saputra and Z. Zhao, "Long term key management architecture for SCADA systems," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 314–319. [Online]. Available: https://ieeexplore.ieee.org/document/8355183

[66] N. Kumar, K. S. Rajpurohit, and Er. G. Srivastava, "Wireless SCADA," *Int. J. Trend Sci. Res. Develop.*, vol. 3, no. 3, pp. 362–364, Apr. 2019, doi: 10.31142/ijtsrd22790.

[67] B. Spoorthi and D. Harekal, "SCADA security in various industrial sectors," in *Proc. 3rd IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2018, pp. 339–346, doi: 10.1109/rteict42901.2018.9012395.

[68] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1942–1976, 3rd Quart., 2020, doi: 10.1109/comst.2020.2987688.

[69] S. V. Moshko and A. D. Stotckaia, "Principles of SCADA-system development," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Jan. 2018, pp. 937–940, doi: 10.1109/eiconrus.2018.8317243.

[70] M. Segovia, A. R. Cavalli, N. Cuppens, and J. Garcia-Alfaro, "A study on mitigation techniques for scada-driven cyber-physical systems (position paper)," in *Proc. Int. Symp. Found. Pract. Secur.*, Nov. 2018, pp. 257–264, doi: 10.1007/978-3-030-18419-3_17.

[71] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016, doi: 10.1109/access.2016.2549047.

[72] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, "ICS/SCADA system security for CPS," in *Cyber Security for Cyber Physical Systems* (Studies in Computational Intelligence). Cham, Switzerland: Springer, 2018, pp. 89–113, doi: 10.1007/978-3-319-75880-0_5.

[73] National Institute of Standards and Technology NIST. *IoT Devices and Infrastructure Group*. Accessed: May 18, 2022. [Online]. Available: https://www.nist.gov/ctl/smart-connected-systems-division/iot-devices-and-infrastructure-group

[74] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, Feb. 2015. [Online]. Available: https://www.mdpi.com/1424-8220/15/3/4837

[75] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016, doi: 10.1109/jsac.2016.2525418.

[76] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[77] S. D. Grigorescu, G. C. Seritan, B. A. Enache, F. C. Argatu, and F. C. Adochiei, "Open source architecture for iot based SCADA system for smart home," *Sci. Bull. Electr. Eng. Fac.*, vol. 20, no. 1, pp. 33–36, Apr. 2020, doi: 10.2478/sbeef-2020-0107.

[78] M. Zamanlou and M. T. Iqbal, "Development of an economical SCADA system for solar water pumping in Iran," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Sep. 2020, pp. 1–4, doi: 10.1109/iemtronics51293.2020.9216408.

[79] C. N. Oton and M. T. Iqbal, "Low-cost open source IoT-based SCADA system for a BTS site using ESP32 and Arduino IoT cloud," in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Dec. 2021, pp. 0681–0685, doi: 10.1109/uemcon53757.2021.9666691.

[80] L. O. Aghenta and M. T. Iqbal, "Low-cost, open source IoT-based SCADA system design using thinger.IO and ESP32 thing," *Electronics*, vol. 8, no. 8, p. 822, Jul. 2019, doi: 10.3390/electronics8080822.

[81] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," *Appl. Soft Comput.*, vol. 71, pp. 66–77, Oct. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1568494618303491

[82] T. Baker, M. Asim, Á. MacDermott, F. Iqbal, F. Kamoun, B. Shah, O. Alfandi, and M. Hammoudeh, "A secure fog-based platform for SCADA-based IoT critical infrastructure," *Softw., Pract. Exper.*, vol. 50, no. 5, pp. 503–518, May 2020, doi: 10.1002/spe.2688.

[83] R. Aldmour, P. Burnap, and M. Lakoju, "Risk assessment methods for converged IoT and SCADA systems: Review and recommendations," in *Proc. Living Internet Things (IoT)*, 2019, p. 6, doi: 10.1049/cp.2019.0130.

[84] IoT.nxt. (Jul. 2018). *IoT and SCADA: Is One Going to Replace the Other?*. Accessed: May 25, 2022. [Online] Available: https://www.iotnxt.com/iot-or-scada/

[85] R. Amudhevalli and D. T. Sivakumar, "Fourth industrial revolution–implementing fourth generation SCADA with the revolutionizing technology of Internet of Things," *Int. J. Eng. Appl. Sci. Technol.*, vol. 4, no. 5, pp. 199–201, Oct. 2019, doi: 10.33564/ijeast.2019.v04i05.030.

[86] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ICS) security," NIST, Gaithersburg, MD, USA, Tech. Rep. 800-82, Jul. 2015.

[87] R. Dhobley and C. Abhay, "Comparative analysis of traditional SCADA systems and IoT implemented SCADA," *Int. J. Advance Res., Ideas Innov. Technol.*, vol. 3, no. 6, pp. 1217–1219, 2017.

[88] M. Moghaddam, M. N. Cadavid, C. R. Kenley, and A. V. Deshmukh, "Reference architectures for smart manufacturing: A critical review," *J. Manuf. Syst.*, vol. 49, pp. 215–225, Oct. 2018, doi: 10.1016/j.jmsy.2018.10.006.

[89] M. Kinoshita, "Japan on the new industrial revolution (NIR): Direction and its global implication for inclusive and sustainable industrial development," Graduate School Public Policy, Univ. Tokyo, Tokyo, Japan, Tech. Rep., Mar. 2019.

[90] D. Allen. (Feb. 2021). Japan: How Its Industries Have Transitioned Into 2021. Medical Expo E-Magazine. [Online]. Available: https://emag.medicalexpo.com/japan-how-its-industries-have-transitioned-into-2021/

[91] F. Kaiser, S. Jia, D. Zheng, and E. Tao. (Sep. 2020). Hidden Truth Of China'S Industrial Automation. InterChina Insights. [Online]. Available: http://www.interchinapartners.com/site/insightDetail/156

[92] D. Cao. (Dec. 2016). What Is China's Smart Manufacturing Strategy? ARC Advisory Group. [Online]. Available: https://www.arcweb.com/industry-best-practices/what-chinas-smart-manufacturing-strategy

[93] S. Wei, J. Hu, Y. Cheng, Y. Ma, and Y. Yu, "The essential elements of intelligent manufacturing system architecture," in *Proc. 13th IEEE Conf. Autom. Sci. Eng. (CASE)*, Aug. 2017, pp. 1006–1011, doi: 10.1109/COASE.2017.8256234.

[94] Manufacturing USA. *Driving Innovation in U.S. Manufacturing*. Accessed: Apr. 28, 2022. [Online] Available: https://www.manufacturingusa.com/

[95] J. F. Sargent Jr., (Jan. 2017). The National Network for Manufacturing Innovation (R44371). United States Congress, Congressional Research Service. [Online] Available: https://crsreports.congress.gov/product/details?prodcode=R44371

[96] *National Network for Manufacturing Innovation Program Strategic Plan*, U.S. Federal Government, Executive Office of the President of the United States (EOP), Washington, DC, USA, Feb. 2016.

[97] IBM. *Industry 4.0 Architecture for Manufacturing*. Accessed: Apr. 10, 2022. [Online] Available: https://www.ibm.com/cloud/architecture/architectures/industry-40/reference-architecture

[98] P. Kiradjiev. (Apr. 2017). *Announcing the IoT Industrie 4.0 Reference Architecture*. [Online] Available: https://www.ibm.com/cloud/blog/announcements/iot-industrie-40-reference-architecture

[99] *The Industrial Internet of Things Volume G1: Reference Architecture*, Industrial Internet Consortium IIC, Boston, MA, USA, Jun. 2019. [Online] Available: https://www.iiconsortium.org/IIRA.htm

[100] Federal Ministry for Economic Affairs and Climate Action BMWK; Federal Ministry of Education, and Research BMBF. *Plattform Industrie 4.0*. Accessed: Apr. 28, 2022. [Online]. Available: https://www.plattform-i40.de/IP/Navigation/EN/Home/home.html

[101] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster, "Recommendations for implementing the strategic initiative industrie 4.0: Securing the future of German manufacturing industry; final report of the industrie 4.0 working group," Nat. Acad. Sci. Eng., Frankfurt, Germany, Tech. Rep., Apr. 2013.

[102] *Enterprise-Control System Integration—Part 1: Models and Terminology*, Standard ISO/IEC 62264-1:2013, May 2013.

[103] *Industrial-Process Measurement, Control and Automation–Life-Cycle-Management for Systems and Components*, document IEC 62890:2020, Jul. 2020.

[104] *Batch Control—Part 4: Batch Production Records*, document IEC 61512-4:2009, Oct. 2009.

[105] *Smart Manufacturing–Reference Architecture Model Industry 4.0 (RAMI4.0)*, document IEC PAS 63088:2017, Mar. 2017.

[106] R. Heidel, M. Hoffmeister, M. Hankel, U. Döbrich, and B. Verlag, *Industrie 4.0: The Reference Architecture Model RAMI 4.0 and the Industrie 4.0 Component*, 1ST ed. Berlin, Germany: Beuth Verlag, Oct. 2019

[107] *ISA-TR-88.95.01, Using ISA-88 and ISA-95 Together*, International Society of Automation ISA, Research Triangle, NC, USA, 2008.

[108] Federal Ministry for Economics Affairs and Climate Action (BMWI) & Federal Ministry of Education and Research (BMBF), Plattform Industrie 4.0. (Aug. 2018). *Reference Architectural Model Industrie 4.0 (RAMI4.0)—An Introduction*. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.html

[109] *Industrial-Process Measurement, Control and Automation—Digital Factory Framework—Part 1: General Principles*, document IEC 62832-1:2020, Oct. 2020.

[110] German Electrical and Electronic Manufacturers Association (ZVEI), "Examples of the asset administration shell for industrie 4.0 components—Basic part," ZVEI, Frankfurt, Germany, White Paper, Apr. 2017.

[111] ZVEI and Plattform Industrie 4.0., "Plattform industrie 4.0—Details of the asset administration shell—Part 2," Federal Ministry Econ. Affairs, Berlin, Germany, Tech. Rep. 1.0RC02, Nov. 2021.

[112] E. Y. Nakagawa, P. O. Antonino, F. Schnicke, R. Capilla, T. Kuhn, and P. Liggesmeyer, "Industry 4.0 reference architectures: State of the art and future trends," *Comput. Ind. Eng.*, vol. 156, Jun. 2021, Art. no. 107241, doi: 10.1016/j.cie.2021.107241.

[113] S. R. Bader, M. Maleshkova, and S. Lohmann, "Structuring reference architectures for the industrial Internet of Things," *Future Internet*, vol. 11, no. 7, p. 151, Jul. 2019, doi: 10.3390/fi11070151.

[114] P. Adolphs et al., "The structure of the administration shell: Trilateral perspectives from France, Italy and Germany," Federal Ministry for Econ. Affairs Energy (BMWi), Berlin, Germany, Tech. Rep., Mar. 2018. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/hm-2018-trilateral-e-coop.html

[115] J. Gayko, S. Wei, M. Hankel, F. Schewe, and M. Hoffmeister, "Alignment report for reference architectural model for industrie 4.0/ intelligent manufacturing system architecture," Federal ministry of economic affairs and energy (BMWi), Berlin, Apr. 2018.

[116] Standardization Council Industrie 4.0 (SCI40). *German—Japanese Cooperation—Standardization Council Industrie 4.0*. Accessed: Apr. 5, 2022. [Online] Available: https://www.sci40.com/english/cooperations/germany-japan/

[117] F. Kimura, T. Baba, H. Komoto, K. Nakashima, S. Oda, Y. Nonaka, M. Hoffmeister, J. Gayko, Y. Leboucher, U. Löwen, and I. Weber, "Germany-Japan common strategy for industrie 4.0 and industrial Internet of Things (IIoT)," Standardization Council Industrie 4.0, Robot Revolution and Ind. IoT initiative, Frankfurt am Main, Germany, Tech. Rep., Oct. 2020.

[118] A. Rojko, "Industry 4.0 concept: Background and overview," *Int. J. Interact. Mobile Technol.*, vol. 11, no. 5, pp. 77–90, Jul. 2017, doi: 10.3991/IJIM.V11I5.7072.

[119] K. Lichtblau, V. Stich, R. Bertenrath, M. Blum, M. Bleider, A. Millack, K. Schmitt, E. Schmitz, and M. Schröter, "Industrie 4.0 readiness," Cologne Inst. Econ. Res. Aachen Univ., Aachen, Cologne, Tech. Rep., Dec. 2015.

[120] OPC Foundation. *I4AAS—Industrie 4.0 Asset Administration Shell*. Accessed: May 10, 2022. [Online] Available: https://opcfoundation.org/marketscollaboration/i4aas/

[121] P. F. S. Melo, E. P. Godoy, P. Ferrari, and E. Sisinni, "Open source control device for industry 4.0 based on RAMI 4.0," *Electronics*, vol. 10, no. 7, p. 869, Apr. 2021, doi: 10.3390/electronics10070869.

[122] P. F. S. de Melo and E. P. Godoy, "Controller interface for industry 4.0 based on RAMI 4.0 and OPC UA," in *Proc. II Workshop Metrol. Ind. 4.0 IoT (MetroInd4.0 IoT)*, Jun. 2019, pp. 229–234, doi: 10.1109/metroi4.2019.8792837.

[123] A. Luder, M. Schleipen, N. Schmidt, J. Pfrommer, and R. Henssen, "One step towards an industry 4.0 component," in *Proc. 13th IEEE Conf. Autom. Sci. Eng. (CASE)*, Aug. 2017, pp. 1268–1273, doi: 10.1109/coase.2017.8256275.

[124] A. Seif, C. Toro, and H. Akhtar, "Implementing industry 4.0 asset administrative shells in mini factories," *Procedia Comput. Sci.*, vol. 159, pp. 495–504, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919313870, doi: 10.1016/j.procs.2019.09.204.

[125] D. A. Bauer and JJ. Mäkiö, "Hybrid cloud–architecture for administration shells with RAMI4.0 using actor4j," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, Jul. 2019, pp. 79–86, doi: 10.1109/indin41052.2019.8972075.

[126] P. Adolphs. (Jun. 2015). *RAMI 4.0 an Architectural Model for Industrie 4.0*. Berlin. [Online]. Available: https://www.omg.org/news/meetings/tc/berlin-15/special-events/mfg-presentations/adolphs.pdf

[127] Plattform Industrie 4.0 and ZVEI, "Part 2-interoperability at runtime—Exchanging information via application programming interfaces (version 1.0RC02)," Federal Ministry For Economic Affairs and Energy (BMWi), Berlin, Germany, Tech. Rep. 1.0RC02, Nov. 2021.

[128] A. Ahmadi, C. Cherifi, V. Cheutet, and Y. Ouzrout, "Recent advancements in smart manufacturing technology for modern industrial revolution: A survey," *J. Eng. Inf. Sci. Stud.*, 2020.

[129] S. Mach, F. Ubis, A. Honka, P. Heikkilä, and E. Kaasinen, "Empowering and participatory adaptation of factory automation to fit for workers," Enabling Technologies, European Comission: Research and Innovation, Brussels, Belgium, Tech. Rep. D1.1, Mar. 2017.

[130] P. Adolphs, S. Auer, H. Bedenbender, M. Billmann, M. Hankel, R. Heidel, M. Hoffmeister, H. Huhle, M. Jochem, and M. Kiele-Dunsche, "Structure of the administration shell: Continuation of the development of the reference model for the industrie 4.0 component," Federal Ministry for Econ. Affairs Energy (BMWi), Berlin, Germany, Tech. Rep., 2016.

[131] International society of automation (ISA). *ISA112 SCADA Systems Standards Committee*. Accessed: Apr. 20, 2022. [Online] Available: https://www.isa.org/standardsand-publications/isa-standards/isa-standards-committees/isa112

[132] Platform I4.0-RRI-SCI, "The common strategy on international standardization in field of the Internet of Things/industrie 4.0," Platform Industrie 4.0 Publication, Berlin, Germany, Tech. Rep., Mar. 2017.

[133] Standardization Council Industrie 4.0, "German standardization roadmap industrie 4.0 (version 4)," German Commission Electrotech., Electron., Inf. Technol. DIN VDE, Frankfurt am Main, German Inst. Standardization (DIN), Berlin, Germany, Tech. Rep., Mar. 2020.

[134] S.-W. Lin, B. Murphy, E. Clauer, U. Loewen, R. Neubert, G. Bachmann, and M. Hankel, "Architecture alignment and interoperability an industrial internet consortium and plattform Industrie 4.0 joint whitepaper," Industrial Internet Consortium (IIC) and Plattform Industrie 4.0, Boston, MA, USA, Tech. Rep. IIC:WHT:IN3:V1.0:PB:20171205, Dec. 2017.

[135] BITKOM, VDMA and ZVEI, "Implementation strategy industrie 4.0 report on the results of the industrie 4.0 platform," Plattform Industrie 4.0, Berlin, Germany, Tech. Rep., Jan. 2016.

[136] *Ivra Next: Strategic Implementation Framework of Industrial Value Chain for Connected Industries*, Industrial Value Chain Initiative, Tokyo, Japan, Mar. 2018.

[137] *Strategic Implementation for Connected Industries-IVRA Next*, Industrial Value Chain Initiative, Tokyo, Japan, Nov. 2017.

[138] C. H. Young, W. P. Lee, and C. Lazarus, "Industry 4.0 reference architectural models: Critical review and opportunities," *Int. J. Adv. Res. Eng. Innov.*, vol. 3, no. 4, pp. 40–49, Dec. 2021.

[139] *Industrial Valuechain Initiative: Ivi Component*, Industrial Value Chain Initiative (IVI), Tokyo, Japan, 2020.

[140] Industrial Value chain Initiative (IVI). *Industrial Value Chain Initiative: Advanced Study Group (ASG)*, Accessed: Mar. 28, 2022. [Online] Available: https://ivi.org/en/activities/asg/

[141] Industrial Value chain Initiative (IVI). *Industrial Value Chain Initiative: Reference Model as a Loose Standard*. Accessed: Mar. 28, 2022. [Online]. Available: https://iv-i.org/en/2019/11/02/english-5-reference-model-as-a-loose-standard-first-published-in-japanese-in-june-2014/

[142] Y. Nonaka, "Clarifying and assisting smart manufacturing standardization with URM-MM," in *Proc. 3rd RRI Int. Symp. Connected Industries Rep.*, in Harmonizing Smart Manufacturing Standards with Usecases, Apr. 2022. [Online]. Available: https://www.jmfrri.gr.jp/english/info/791.html

[143] K. Takahashi, Y. Ogata, and Y. Nonaka, "A proposal of unified reference model for smart manufacturing," in *Proc. 13th IEEE Conf. Autom. Sci. Eng. (CASE)*, Aug. 2017, pp. 964–969, doi: 10.1109/coase.2017.8256228.

[144] M. Bauer, M. Boussard, N. Bui, F. Carrez, P. Giacomin, S. Haller, E. Ho, C. Jardak, J. De Loof, C. Magerkurth, S. Meissner, A. Nettsträter, and A. Olivereau, "Internet of Things—Architecture IoT-A deliverable D1.3—Updated reference model for IoT V1.5," Seventh Framework Program, European Commission, Brussels, Belgium, Tech. Rep. 257521, 2012.

[145] A. Serbanati, A. Olivereau, A. Bassi, A. Nettstraeter, A. Castellani, K. Koutsopoulos, P. Giacomin, M. Rossi, and R. Bonetto, "IoT-A Internet of Things architecture WP3—Protocol suite," Seventh framework Program, European Commission, Brussels, Belgium, Tech. Rep. IOT-A_WP3_D3.3, 2012.

[146] S. Debortoli, K. Sperner, C. Magerkurth, D. Dobre, and S. Meissner, "Internet of Things architecture IoT-A project deliverable D2.3—Orchestration of distributed IoT service interactions," Seventh Framework Program, European Commission, Brussels, Belgium, Tech. Rep. 257521, 2012.

[147] A. Serbanati, A. S. Segura, A. Oliverau, Y. B. Saied, N. Gruschka, D. Gessner, and F. Gomez-Marmol, "Internet of Things architecture IoT-A project deliverable D4.2 concepts and solutions for privacy and security in the resolution infrastructure," European commission, Seventh Framework Program, Brussels, Belgium, Tech. Rep. 257521, 2012.

[148] M. Bauer, M. Boussard, N. Bui, F. Carrez, P. Giacomin, S. Haller, E. Ho, C. Jardak, J. De Loof, C. Magerkurth, S. Meissner, A. Nettsträter, A. Olivereau, and J. W. Walewski, "Internet of Things—Architecture IoT-A deliverable D1.4—Converged architectural reference model for the IoT V2.0," European commission, Seventh Framework Program, Brussels, Belgium, Tech. Rep. 257521, 2012.

[149] IoT-A and Seventh Framework Program. *IoT-A: Internet of Things Architecture—Unified Requirement List*. Accessed: Apr. 9, 2022. [Online] Available: https://www.iota.eu/public/requirements/

[150] ARC Advisory Group. *Arc Advisory Group: How To Standardize Smart Manufacturing the China Way*, Accessed: Apr. 10, 2022. [Online] Available: https://www.arcweb.com/industry-best-practices/how-standardizesmart-manufacturing-china-way

[151] Standardization Administration of the P.R.C. (SAC). *Standardization Administration of the P.R.C. (SAC)*. Accessed: Apr. 10, 2022. [Online] Available: http://www.sac.gov.cn/sacen/Standards/Release/202102/

[152] The PRC Ministry Of Industry and Information Technology (MOST) and The standardization administration of China (SAC), "Guidelines for the construction of a national smart manufacturing standards system," Beijing, China, Tech. Rep., Nov. 2021.

[153] R. Li, S. Wei, and J. Li, "Study on the application framework and standardization demands of AI in intelligent manufacturing," in *Proc. Int. Conf. Artif. Intell. Adv. Manuf. (AIAM)*, 2019, pp. 604–607, doi: 10.1109/AIAM48774.2019.00125.

[154] P. Kiradjiev. (Apr. 2017). *Announcing the IoT Industrie 4.0 Reference Architecture*. Accessed: Mar. 25, 2022. [Online]. Available: https://www.ibm.com/cloud/blog/announcements/iot-industrie-40-reference-architecture

[155] Industry IoT Consortium. *Industry IoT Consortium—About us.* Accessed: Mar. 25, 2022. [Online] Available: https://www.iiconsortium.org/about-us/

[156] Industry IoT Consortium. *Keeping Pace With the Rapid Changes in Industrial IoT*. Accessed: Mar. 25, 2022. [Online] Available: https://www.iiconsortium.org/wc-industry/

[157] C. Baudoin, E. Bournival, M. Buchheit, E. Simmon, and B. Zarkout, "Industry Internet of Things vocabulary," Industry IoT Consortium, Boston, MA, USA, Tech. Rep. 3.00-2022-03-22, 2022.

[158] Object Management Group. *Popular OMG Standards*. Accessed: Mar. 26, 2022. [Online]. Available: https://www.omg.org/about/omg-standards-introduction.htm

[159] M. Bauer, N. Bui, P. Giacomin, N. Gruschka, S. Haller, E. Ho, R. Kernchen, L. Mario, J. De, S. Meissner, A. S. Segura, J. W. Walewski, and S. Haller, "Internet-of-Things architecture IoT-A project deliverable D1.2—Initial architectural reference model for IoT," Seventh framework program, European commission, Brussels, Belgium, Tech. Rep. 257521, 2011.

[160] OASIS. *Oasis—Open Standards*. Accessed: Mar. 28, 2022. [Online] Available: https://www.oasisopen.org/standards/

[161] World Wide Web Consortium. *W3C Standards*. Accessed: Mar. 28, 2022. [Online] Available: https://www.w3.org/standards/

[162] S. Meissner, D. Dobre, M. Thoma, and G. Martin, "Internet of Things architecture IoT-A project deliverable D2.1—Resource description specification," Seventh Framework Program, European commission, Brussels, Belgium, Tech. Rep. 257521, 2012.

[163] A. Bondza, C. Eck, R. Heidel, M. Reigl, and S. Wenzel, "Eclss white paper: Toward smart manufacturing with data and semantics," Ecl@sse. V, Munich, White Paper, Feb. 2018. [Online]. Available: https://www.messe.de/apollo/hannover_messe_2020/obs/Binary/A1003867/1003867_02139271.pdf

[164] ECLASS. *Eclass Homepage: The Current Version*. Accessed: Mar. 28, 2022. [Online]. Available: https://eclass.eu/en

[165] D&TS. ECLASS—The Standard for Master Data and Digitalization. Data services & IT-Solutions. Accessed: Mar. 29, 2022. [Online]. Available: https://www.dundts.com/en/eclass

[166] B. Miller and D. C. Rowe, "A survey of SCADA and critical infrastructure incidents," in *Proc. ACM Res. Inf. Technol.*, Oct. 2012, pp. 51–56, doi: 10.1145/2380790.2380805.

[167] J. Prinsloo, S. Sinha, and B. von Solms, "A review of industry 4.0 manufacturing process security risks," *Appl. Sci.*, vol. 9, no. 23, p. 5105, Nov. 2019, doi: 10.3390/app9235105.

[168] S. Al-Rabiaah, "The 'Stuxnet' virus of 2010 as an example of a 'APT' and Its 'recent' variances," in *Proc. 21st Saudi Comput. Soc. Nat. Comput. Conf. (NCC)*, 2018, pp. 1–5, doi: 10.1109/NCG.2018.8593143.

[169] S. Alelyani and G. R. H. Kumar, "Overview of Cyberattack on Saudi organizations," *J. Inf. Secur. Cybercrimes Res.*, vol. 1, no. 1, pp. 32–39, Jun. 2018, doi: 10.26735/16587790.2018.004.

[170] C. Bronk and E. Tikk-Ringas, "The cyber attack on Saudi aramco," *Survival, Global Politics Strategy*, vol. 55, no. 2, pp. 81–96, May 2013, doi: 10.1080/00396338.2013.784468.

[171] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Eng. (CPRE)*, 2017, pp. 1–8, doi: 10.1109/CPRE.2017.8090056.

[172] A. Banga, D. Gupta, and R. Bathla, "Towards a taxonomy of cyber attacks on scada system," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, May 2019, pp. 343–347, doi: 10.1109/iccs45141.2019.9065534.

[173] S. Ghosh and S. Sampalli, "A urvey of ecurity in SCADA etworks: Current ssues and uture hallenges," in *IEEE Access*, vol. 7, pp. 135812–135831, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8753583

[174] C. C. Davidson, T. R. Andel, M. Yampolskiy, T. J. McDonald, B. W. Glisson, and T. Thomas, "On scada PLC and fieldbus cybersecurity," in *Proc. 13th Int. Conf. Cyber Warfare Secur. (ICCWS)*, Washington, DC, USA, Mar. 2018, pp. 140–148.

[175] S. D. D. Anton, D. Fraunholz, D. Krohmer, D. Reti, D. Schneider, and H. D. Schotten, "The global state of security in industrial control systems: An empirical analysis of vulnerabilities around the world," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17525–17540, Dec. 2021, doi: 10.1109/jiot.2021.3081741.

[176] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2248–2294, 4th Quart., 2021, doi: 10.1109/comst.2021.3094360.

[177] C. Ekisa, D. O. Briain, and Y. Kavanagh, "An open-source testbed to visualise ICS cybersecurity weaknesses and remediation strategies—A research agenda proposal," in *Proc. 32nd Irish Signals Syst. Conf. (ISSC)*, Jun. 2021, pp. 1–6, doi: 10.1109/issc52156.2021.9467852.

[178] S. Potluri, C. Diedrich, S. R. Roy Nanduru, and K. Vasamshetty, "Development of injection attacks toolbox in MATLAB/Simulink for attacks simulation in industrial control system applications," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, Jul. 2019, pp. 1192–1198, doi: 10.1109/indin41052.2019.8972171.

[179] R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, "Stealthy attack against redundant controller architecture of industrial cyber-physical system," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9783–9793, Dec. 2019, doi: 10.1109/jiot.2019.2931349.

[180] T. Choi, G. Bai, R. K. L. Ko, N. Dong, W. Zhang, and S. Wang, "An analytics framework for heuristic inference attacks against industrial control systems," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 827–835, doi: 10.1109/trustcom50675.2020.00112.

[181] S. Kendzierskyj and H. Jahankhani, "The role of blockchain in supporting critical national infrastructure," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability (ICGS)*, Jan. 2019, pp. 208–212, doi: 10.1109/icgs3.2019.8688026.

[182] L. Deng, Y. Peng, C. Liu, X. Xin, and Y. Xie, "Intrusion detection method based on support vector machine access of modbus TCP protocol," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Dec. 2016, pp. 380–383, doi: 10.1109/ithings-greencom-cpscom-smartdata.2016.90.

[183] F. A. Osman, M. Y. M. Hashem, and M. A. R. Eltokhy, "Secured cloud SCADA system implementation for industrial applications," *Multimedia Tools Appl.*, vol. 81, no. 7, pp. 9989–10005, Mar. 2022, doi: 10.1007/s11042-022-12130-9.

[184] T. Alves, T. Morris, and S.-M. Yoo, "Securing SCADA applications using OpenPLC with end-to-end encryption," in *Proc. 3rd Annu. Ind. Control Syst. Secur. Workshop*, Dec. 2017, pp. 1–6, doi: 10.1145/3174776.3174777.

[185] E. Winter and M. Rademacher, "Fuzzing of SCADA protocols used in smart grids," *Energy Informat.*, vol. 3, no. 2, pp. 1–3, Oct. 2020. [Online]. Available: https://energyinformatics.springeropen.com/articles/10.1186/s42162-020-00113-9#Sec5

[186] A. Tidrea, A. Korodi, and I. Silea, "Cryptographic considerations for automation and SCADA systems using trusted platform modules," *Sensors*, vol. 19, no. 19, p. 4191, Sep. 2019, doi: 10.3390/s19194191.

[187] *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability*, U.S. Homeland Security, Washington, DC, USA, 2009.

[188] ENISA, "Guideline on security measures under the EECC," in *The European Union Agency for Cybersecurity*, 4th ed. Jul. 2021, doi: 10.2824/44013.

[189] L. Thames and D. Schaefer, "Cybersecurity for industry 4.0: Analysis for design and Manufacturing," Springer, Cham. Switzerland, 2017. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-50660-9_3

[190] E. Hernández, P. Senna, D. Silva, R. Rebelo, A. C. Barros, and C. Toscano, "Implementing RAMI4.0 in production—A multi-case study," in *Progress in Digital and Physical Manufacturing* (Lecture notes in mechanical engineering), H. A. Almeida and J. C. Vasco, Eds. Cham, Switzerland: Springer, 2019. [Online]. Available: https://repositorio.inesctec.pt/items/477b6d4a-e801-4253-bcb8-c2b26e283cb9 and https://www.springerprofessional.de/en/implementing-rami4-0-in-production-a-multi-case-study/17219972

[191] Iinternational Society of Automation (ISA). *ISA112, SCADA Systems*. Accessed: Mar. 28, 2022. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa112

[192] J. Müller, "Enabling technologies for industry 5.0: Results of a workshop with Europe's technology leaders," Luxembourg, Eur. Commission, Directorate-General Res. Innov., Brussels, Belgium, Tech. Rep. KI-04-20-494-EN-N, Sep. 2020. Accessed: Mar. 29, 2022. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/8e5de100-2a1c-11eb-9d7e-01aa75ed71a1/language-en

[193] Meticulous Research. *Top 10 Companies in SCADA Market*. Accessed: Apr. 20, 2022. [Online]. Available: https://meticulousblog.org/top-10-companies-in-scada-market/

[194] Businesswire. *Global Scada Market 2017–2021*. Accessed: Apr. 20, 2022. [Online]. Available: https://www.businesswire.com/news/home/20170803005484/en/Global-SCADA-Market-2017-2021

[195] Automation Forum. *Leading 12 Scada Software*, Accessed: Apr. 20, 2022. [Online]. Available: https://automationforum.co/leading-12-scada-software/

[196] Precedence Research. *SCADA Market Size*. Accessed: Apr. 21, 2022. [Online]. Available: https://www.precedenceresearch.com/scada-market

[197] Businesswire. *Global SCADA Market 2017–2021*. Accessed: Apr. 21, 2022. [Online]. Available: https://www.businesswire.com/news/home/20170803005484/en/Global-SCADA-Market-2017-2021

[198] Meticulous Research. *Industrial IoT Market: Global Opportunity Analysis and Industry Forecast (2022–2029)*. Accessed: Apr. 21, 2022. [Online]. Available: https://www.meticulousresearch.com/product/industrial-iot-market-5102

[199] Inductive Automation. *Inductive Automation: Ignition Industrial Application Platform*. Accessed: Sep. 13, 2022. [Online]. Available: https://inductiveautomation.com/

[200] Siemens. *Totally Integrated Automation Portal' Automation Software, Siemens Global*. Accessed: Apr. 21, 2022. [Online]. Available: https://new.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal.html
[201] CopaData. *Zenon Release and Support Cycles*. Accessed: Apr. 22, 2022. [Online]. Available: https://www.copadata.com/en/support-services/release-support-cycles/
[202] InSource Solutions. *TN Ww121 Aveva Software Versions Index*. Accessed: Apr. 22, 2022. [Online]. Available: https://knowledge.insourcess.com/Supporting_Technologies/Wonderware/Tech_Notes/TN_WW121_Aveva_Software_Versions_Index
[203] A. G. Siemens. *Industry Support Siemens: Simatic Step 7 Basic V14 SP1—Product Details*. Accessed: Apr. 25, 2022. [Online]. Available: https://support.industry.siemens.com/cs/pd/752688?pdti=pi&dl=en&lc=en-WW
[204] *Report on the 5th Science and Technology Basic Plan*, Council Sci., Technol. Innov. Cabinet Office, Government Japan, Japan, Dec. 2015. [Online]. Available: https://www8.cao.go.jp/cstp/kihonkeikaku/5basicplan_en.pdf
[205] Ministry of Economy Trade and Industry (METI). *Connected Industries*. Government of Japan. Accessed: Apr. 28, 2022. [Online]. Available: https://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html
[206] European Commission. *A Europe fit for the Digital Age*. Accessed: Apr. 28, 2022. [Online]. Available: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en
[207] European Commission. *Industry 5.0*. Accessed: May 10, 2022. [Online]. Available: https://ec.europa.eu/info/research-and-innovation/research-area/industrial-research-and-innovation/industry-50_en
[208] M. Breque, L. De Nul, and A. Petridis, "Industry 5.0 towards a sustainable, human-centric and resilient European industry," European Commission, Brusseles, Tech. Rep. KI-BD-20-021-EN-N, 2021.
[209] A. Akundi, D. Euresti, S. Luna, W. Ankobiah, A. Lopes, and I. Edinbarough, "State of industry 5.0—Analysis and identification of current research trends," *Appl. Syst. Innov.*, vol. 5, no. 1, pp. 1–14, 2022, doi: 10.3390/asi5010027.
[210] M. M. Nair, A. K. Tyagi, and N. Sreenath, "The future with industry 4.0 at the core of society 5.0: Open issues, future opportunities and challenges," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–7, doi: 10.1109/iccci50826.2021.9402498.
[211] H. J. Anderson, J. E. Baur, J. A. Griffith, and M. R. Buckley, "What works for you may not work for (Gen)me: Limitations of present leadership theories for the new generation," *Leadership Quart.*, vol. 28, no. 1, pp. 245–260, Feb. 2017, doi: 10.1016/j.leaqua.2016.08.001.
[212] L. M. Finkelstein, E. B. King, and E. C. Voyles, "Age metastereotyping and cross-age workplace interactions: A meta view of age stereotypes at work," *Work, Aging Retirement*, vol. 1, no. 1, pp. 26–40, Jan. 2015, doi: 10.1093/workar/wau002.
[213] M. D. M. Alonso-Almeida, F. C. Fernández de Navarrete, and J. Rodriguez-Pomeda, "Corporate social responsibility perception in business students as future managers: A multifactorial analysis," *Bus. Ethics, A Eur. Rev.*, vol. 24, no. 1, pp. 1–17, Jan. 2015, doi: 10.1111/beer.12060.
[214] T. Yamane and S. Kaneko, "Is the younger generation a driving force toward achieving the sustainable development goals? Survey experiments," *J. Cleaner Prod.*, vol. 292, Apr. 2021, Art. no. 125932, doi: 10.1016/j.jclepro.2021.125932.
[215] T. Obradović, B. Vlačić, and M. Dabić, "Open innovation in the manufacturing industry: A review and research agenda," *Technovation*, vol. 102, Apr. 2021, Art. no. 102221, doi: 10.1016/j.technovation.2021.102221.

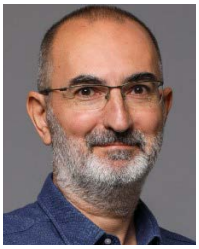
MLADEN ŠVERKO received the B.Sc. degree in marine engineering from the Faculty of Maritime Studies, University of Rijeka, Croatia, in 1996, and the B.Sc. and M.Sc. degrees in informatics from the Faculty of Informatics, Juraj Dobrila University of Pula, Croatia, in 2019 and 2021, respectively. He is currently pursuing the Ph.D. degree in electrical engineering and computing with the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia.

He has been with Danieli-Systec (part of Danieli & C. S.p.A.), since 2002, working on the design, development and commissioning of large-scale SCADA systems deployed worldwide. He specializes in supervisory control and software engineering for the steel industry and medium voltage central monitoring and control systems. In a period of two decades, he participated in more than 50 projects of development and revamping of the industrial control systems of steel plant facilities.

TIHANA GALINAC GRBAC (Member, IEEE) received the M.Sc. and Ph.D. degrees from the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia, in 2005 and 2009, respectively.

She was at Ericsson Nikola Tesla (ETK), Zagreb, Croatia, and was actively involved in the Ericsson Core Network development. The eight years of experience in Research and Development projects developing large scale complex software system that is evolutionary developed by globally distributed teams have strongly influenced and motivated her research. She is a Full Professor of computer science with the Juraj Dobrila University of Pula, Croatia, and the Head of the Software Engineering and Information Processing Laboratory (SEIP Lab), which she established at the Faculty of Engineering, University of Rijeka, Croatia, in 2012 and at the Juraj Dobrila University of Pula, in 2018. She is actively involved as the leader, management committee member and researcher in a number of research projects funded by European Union, Croatian Government, or industry partners.

Dr. Grbac is a member of ACM and HU MIPRO. She was a recipient of the IEEE Croatian Section Award for Exceptional Contribution to Engineering Education in 2017.



MILJENKO MIKUC (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Zagreb, Croatia, in 1997.

He is currently a Full Professor with the Department of Telecommunications, Faculty of Electrical Engineering and Computing, University of Zagreb. His research interests include digital logic design, network protocols, network simulation, and security.