Chapter 5
Industrial Internet of Things

5.1 Introduction

The Internet of Things (IoT) has already brought a revolution to our understanding of applications in a wide range of human activity. This trend is expected to increase in the near future, as the potential economic impact of IoT is expected to be between 900 billion USD and 2.3 trillion USD on a yearly basis up to 2025 [Man13]. IoT applications are spreading to various sectors including smart energy, manufacturing, agriculture, health, security and safety, smart cities, smart buildings, and smart environment. All these application areas repeat the same basic model: a large number of smart devices, interconnected over wired or wireless media, interacting and coordinating to achieve a goal.

In the industrial environment, the effort for smart factories [Zue10], the Industrie 4.0 strategy [Ind14], the Industrial Internet [GE17], and the European initiative for the Factories of the Future [FoF] have initiated the adoption of IoT in industry with the goals of increasing flexibility and productivity, while reducing production cost. The developing concept is the Industrial IoT (IIoT).

The Industrial Internet of Things is part of the general IoT evolution. However, it faces challenges that are unique and differentiate it from the other systems and services of IoT due to the need to integrate programmable logic controllers (PLC) and supervisory control and data acquisition systems (SCADA). PLC and SCADA systems, together with the related industrial networks that interconnect them, constitute the infrastructure of operational technology (OT), which has traditionally evolved independently from the typical IT technology, because it addresses the needs of systems in the field – industrial floor, energy production facilities, energy distribution networks, etc. – with strong requirements such as continuous operation, safety, real-time operation, etc. The capabilities offered by the emerging IIoT technology pose challenges for the integration of these OT systems with the traditional enterprise IT systems at many levels, from enterprise management to cyber security. For example, enterprise resource planning systems (ERP) need to be expanded to

D. Serpanos, M. Wolf, *Internet-of-Things (IoT) Systems*,
https://doi.org/10.1007/978-3-319-69715-4_5

include manufacturing operations, which are managed currently by manufacturing execution systems (MES) that have grown independently and present significant interoperability challenges to their integration. Clearly, an integrated system that manages the complete enterprise/factory hierarchy, from business processes to sensors, provides significant flexibility and presents new opportunities to enterprises.

Industrial technology is not part only of manufacturing or factories. The maturity of the technology and its cyber-physical control capabilities has spread its use outside traditional factory environments, and now they constitute a significant part of the critical infrastructure at many fronts. Energy production and distribution infrastructure includes OT systems, which are the indispensable infrastructure on which modern smart grids are built. Actually, the energy sector is a high priority in the evolution of IIoT, not only because there is increasing need to consumers for energy, especially in light of the population growth, but also because energy management is a critical factor in the industrial sector and the desired low-cost production of goods and services. In addition to the energy sector, industrial systems are widespread in many other sectors of critical infrastructure, such as water management and transportation.

The interoperability challenges to the convergence of IT and OT are only a part of the challenges in the emerging IIoT. Appropriate architectures need to be developed to build and manage effective IIoT systems, technologies for the design and management of cyber-physical systems, sensors and networks need to be developed, and, importantly, safety and security need to be addressed in a unified way in the context of IIoT. Safety and security are significant challenges, because, traditionally, security has been a concern in the IT sector, while safety has been the major concern in the OT sector. Bringing the two together has brought the realization that safety cannot be achieved without security, while, at the same time, security needs to include technologies that combine dependability and meet strong requirements for real time and low power in many application domains. Although the security issues of industrial control systems have attracted attention in the last decade and standards have been evolving at a much faster pace than in the past, e.g., the ISO/IEC 27000 and the ISA/IEC 62443 families of standards [IEC16, ISA16], there are still significant challenges at the technology, architecture, and management fronts to obtain solutions for the unified IIoT.

In this chapter, we present the concepts and evolution of the IIoT starting from the Industrie 4.0 strategy and proceeding to the Industrial Internet. We describe the IIoT reference architectures as they evolve from the ITU effort to the Industrial Internet Consortium. Finally, we describe some representative challenges in the evolution and implementation of IIoT focusing on the energy sector. As security and safety constitute a significant challenge in IIoT as well as in IoT, in general, we focus on this challenge in the following chapter.

5.2 Industrie 4.0

Industrie 4.0 is a strategic initiative in Germany that targets to bring IoT technologies to the manufacturing and production sectors [Ind14].The goal is to enable Germany to keep a leading role in manufacturing achieving efficient and low-cost production with flexible workflows. The means to achieve this goal is the widespread inclusion of cyber-physical systems in the manufacturing and production processes, in order to insert intelligence in the systems and processes, to enable their high connectivity and communication, and to achieve their coordination into more complex but flexible processes that lead to high-quality, low-cost products.

Industrie 4.0 takes its name from the identification of the new, emerging industry as the fourth revolution of industrial production. It is widely accepted that industrial production to date has gone through three (3) revolutions. The first industrial revolution, between the eighteenth and nineteenth century, is the one where mechanized production facilities were introduced in the production of goods and services, where the required energy was provided by water and steam. Electrical energy was introduced during the second revolution, which led to mass production, as electricity boosted productivity. In the post WWII era, the inclusion of electronics and software, i.e., industrial information technology, to the mechanical and electrical components led to the third revolution that enabled automation at high levels. Currently, many industrial stakeholders believe that we are at the verge of the next, the fourth, industrial revolution, through wide adoption and use of cyber-physical systems that leads not only to even higher levels of automation but enables mass customized manufacturing and production of goods and services, due to the flexibility offered by the easily programmable, configurable, and controllable manufacturing lines.

The effort for Industrie 4.0 is based on the widespread deployment and use of computational and communication resources. The last two decades have been characterized by significant advances in high performance, low-power processors, memories, and communication components that enable efficient processing and networking. These advances have brought significant processing capabilities to a large number of devices that are deployed to consumers or to the field. Smart consumer devices have become norm. Smartphones provide hundreds of applications and enable services ranging from identifying travel and transportation routes to mobile banking and health monitoring. Smart televisions combine and provide various types of entertainment and network services, from customized TV channel control and management to Internet gaming and home device management. Smart home appliances monitor parameters, from environmental temperatures to water and energy consumption, enabling citizens to manage their homes efficiently and effectively leading to the required living quality while reducing operational cost at various fronts.

The large basis of computational resources and connectivity becomes apparent by the published numbers of embedded processors and components that are currently produced. According to [Ind14], the vast majority of produced processors, approximately 98%, are deployed in embedded systems. Deployed semiconductor memory is also growing and expected to grow at 40% year over year in 2017 [Mic17]. Furthermore, the significant advances of wired and wireless networks in the last two decades have led to ubiquitous connectivity, approaching 100% in cities and towns, through different technologies.

The available processing and communication basis leads to an evolving hierarchy of embedded systems and services up to the level of the Internet of Things, Data, and Services. Examples of this evolution can be identified at several application areas. In transportation, for example, embedded systems are widespread controlling functions from car entertainment systems to car seat control. At this level, embedded processors are programmed to control specific, individual parameters, e.g., height and movement in car seats, based on user commands. However, embedded systems in cars are also networked, either within the car system or with the environment, providing networked embedded services; automatic toll payment is one of them where embedded systems in the car and the toll booths communicate with each other, in order to complete the electronic payment transaction of the toll passage. Such payment systems from several tolls, for example, can be further combined in a distributed system that enables traffic and toll management at a wider scale, leading to more effective transportation infrastructure that achieves lower waiting times and fuel costs for travelers as well as lower operational cost and, thus, higher income to transportation management authorities. One can even envision an even higher level of connectivity of such complex transportation systems to smart cities that combine transportation management with additional services, such as energy distribution, civil services, emergency services, etc., as required at different times, locations, and during special events.

The advances of sensor technologies, in addition to the evolution of embedded systems and communication networks, make all these scenarios realistic. Importantly, sensors bridge the gap between the physical world and the digital world, providing increasingly rich information to digital systems and enabling intelligent control of systems and processes. In that respect, manufacturing and industrial automation has been traditionally employing IT technologies with sensors and electromechanical systems, leading the development and deployment of technologies and concepts for intelligent control, systems, and services. Thus, the development of the Industrie 4.0 strategy and the related initiatives comes as a natural evolution step of industrial technologies influencing and being influenced by the advancement of consumer technologies of the Internet of Things.

The smart factory concept embodies the goals of the Industrie 4.0 strategy to a large degree. The concept is based on the hierarchy of cyber-physical systems mentioned above, where smart production systems are interconnected in a multilevel hierarchy to achieve a high degree of automation, targeting flexibility, efficiency, autonomy, resilience, safety, and low cost. Smart machines will be interconnected to establish smart plants, which, in turn, will be combined to provide smart factories. Considering the typical components of manufacturing process, smart factories are targeted to automate efficiently all components and stages. Materials and resources will be managed and introduced in the process efficiently; production processing will be managed in real time minimizing the used resources for the products and the operations, while reconfiguration and reorganization of production processes and customization of products will be feasible in real time and with safety for infrastructure and operators, minimizing environmental impact. Customers will be able to monitor the progress of the development of ordered products, while manufacturers will be optimizing their logistics chains.

5.3 Industrial Internet of Things (IIoT)

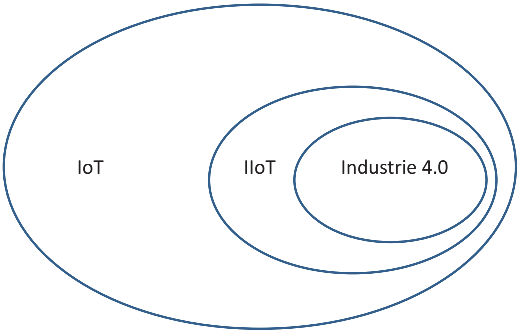
The Industrial Internet of Things (IIoT) has emerged as a general concept of the application of the Internet of Things to the industrial sector. Effectively, it is a generalization of Industrie 4.0, which appears to focus more on industrial process efficiency. The IIoT vision includes all aspects of industrial operations, focusing not only on process efficiency but also on asset management, maintenance, etc.

Considering that IIoT is effectively IoT in the industrial sector and that the Industrie 4.0 concepts are effectively a subset of IIot, as shown in Fig. 5.1, one needs to identify the difference between IoT and IIoT. Although the basic concepts are the same, i.e., interconnected smart devices that enable remote sensing, data collection, processing, monitoring, and control, the parameters that identify the IIoT subset of IoT are the strong requirements for continuous operation and safety as well as the operational technology employed in the industrial sector. As an example, one can consider the difference between a consumer service such as a health monitoring application on a smart watch and an industrial service such as the monitoring of a steam pump. Although both applications collect real-time data, e.g., steps or body temperature in the health application case and pressure or steam volume in the steam pump case, transmit the data, identify events, and provide feedback or commands to operators/consumers and subsystems, clearly, continuous operation and safety place stricter requirements in the steam pump case, where the potential effect of a failure is significantly more catastrophic and may lead to costly operation down time and even human injuries or loss of life.

These characteristics of the industrial sector – technology and requirements – lead to specialized, demanding solutions for technology and services, justifying the focus of the industrial sector on a specialized IoT concept. This has resulted to the strong interest of the industrial sector in the development of specialized concepts, from strategy to application and technology. The conventional business development models that include numerous interdependencies between stakeholders, from supply chains to service promotion, lead also to a strong need for interoperable solutions at many levels, from the device level to services. Thus, there is need for coordinated activities in the evolution to IIoT, which is addressed by consortia, such as the Industrial Internet Consortium [IIC14] that provides significant leadership in this emerging field.

The General Electric company introduced the term *Industrial Internet* in 2012, as a leader of the Industrial Internet of Things, identifying also the technologies of machine-to-machine communication, SCADA, HMI, industrial data analytics, and

Fig. 5.1 IoT, IIoT, and Industrie 4.0 relationship



cybersecurity as the main constituents of the IIoT vision [GE17]. Interestingly, they also calculate the impact of the Industrial Internet to 46% of the global economy, while in the energy sector they calculate an impact of 100% on energy production and 44% on energy consumption globally [GE17].

5.4 IIoT Architecture

The development and deployment of IIoT systems and services require the development of architectures that enable efficient and effective operations as well as interoperability considering the anticipated end-to-end services and the large number of stakeholders involved for devices, cyber-physical systems, communication systems and networks, service providers, and business developers. Thus, significant effort is being spent to develop standards and reference architectures that will be accepted and adopted by the various stakeholders. The International Telecommunication Union (ITU) has addressed this issue, publishing in 2012 the ITU-T Y.2060 recommendation, which introduces a reference architecture for IoT, in general, including explicitly applications that fall in the context of IIoT, such as smart grid, intelligent transportation systems, e-health, etc. [ITU12]. The Industrial Internet Consortium (IIC) has also been working on a reference architecture for IIoT and currently has published Version 1.7 of the Industrial Internet Reference Architecture [IIC17]. This architecture is an elaborated reference architecture, significantly more detailed than the ITU one, addressing all important aspects to all categories of stakeholders. Taking into account the details of both reference models, one can consider the IIC model as a specialized evolution of the ITU model, addressing in more details the important issues of IIoT relatively to the more generic ITU reference model that encapsulates the requirements for the general IoT.

The ITU effort has expanded the communications' vision to include communication of "anything" to the communication concepts of "any time" and "any place." Importantly, it includes all expected applications, including industrial ones, specifically mentioning smart grids and intelligent transport systems among others. As "things," ITU considers physical and virtual objects that are identifiable and able to

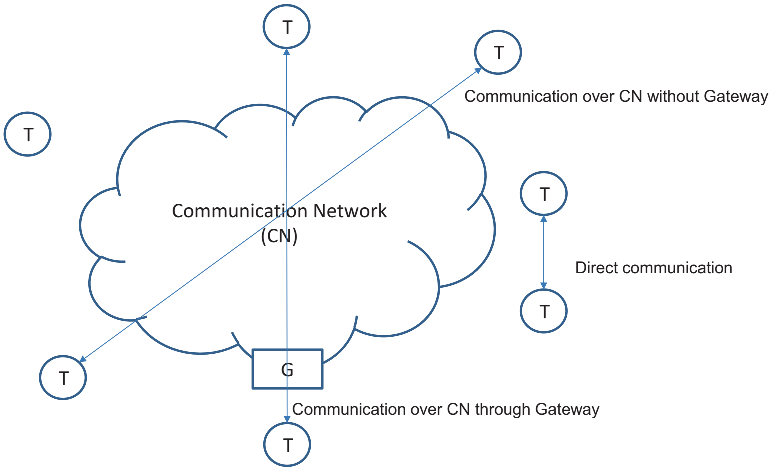

T
T
Communication over CN without Gateway
T
Communication Network
(CN)
T
Direct communication
T
T
G
Communication over CN through Gateway
T

Fig. 5.2 Communication methods for IoT devices

connect to communication networks, while they have related information that is either static or dynamic. Importantly, since communication is a critical part of the whole IoT concept, physical things need to be attached to “devices” that are connected to networks, so that any analog information can be converted to digital and transmitted through the networks. Devices can be simply data-carrying communicating and storing data, data-capturing interacting with the physical objects through reader and writers, sensing and actuating devices, or general-purpose devices with embedded processing and communication resources, such as machines, appliances, and consumer electronic products.

An important issue in the ITU reference model is the communication model among devices. As Fig. 5.2 indicates, the model considers three methods of communication, based on the employment of gateways (G) and the use of the communication network (CN). Devices can communicate without the use of gateways, directly, over local networks, and/or over the communication network, or they can communicate over the communication network exploiting gateways.

The ITU model accommodates fundamental characteristics of IoT that are identified. These fundamental characteristics are interconnectivity, scale, heterogeneity, services for things and the dynamic nature of device information, and connectivity. Interconnectivity is a significant characteristic because “anything” can connect to the global network for any application. As the number of connected devices increases dramatically, scaling becomes a significant parameter that needs to be addressed at all levels of IoT and IIoT; the scaling issue relates not only to communication end points and number of devices but to the size of produced and communicated data as well as their management in terms of storage and processing. The dynamic nature of devices, which turns on and off dynamically or connect and disconnect to networks, will make the landscape more complex and demanding. The open nature of (I)IoT and the large number of stakeholders, in addition to the flexible and long

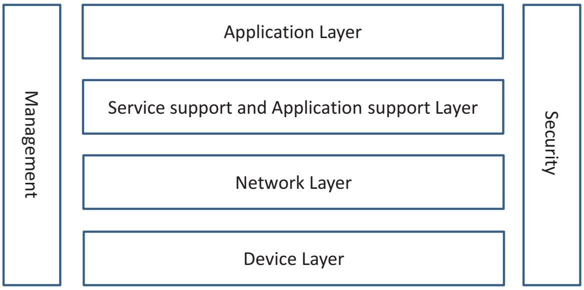


Fig. 5.3 IoT reference model by ITU

supply chains in conventional service provisioning, leads to the need to accommodate heterogeneous "things," devices, platforms, and services. Services for things also need to be addressed appropriately, not only because of the limited resources of many "things" but also because of the requirements of several services for security and safety, including privacy protection and safe actuation that avoids problems and accidents.

The fundamental characteristics of (I)IoT lead to requirements that need to be met by the reference architecture. The main requirements mentioned by ITU include interoperability, identification-based connectivity, autonomy in networking and services, accommodation of location-based services, security and privacy, as well as capabilities for management of things and services, including plug and play.

Figure 5.3 depicts the ITU IoT reference model, which has been introduced to meet the above requirements. It is a typical layered model with four hierarchical layers, specifically device, network, application and service support and finally application layer, and two vertical layers that are crosscutting the four hierarchical layers, defining management and security functions and properties to all hierarchical layers.

The device layer, the lowest in the hierarchy, includes the functionality of devices and communication gateways. Considering the main interest of ITU in communications, the layer describes communication-centered functionality for the devices: (a) devices that transmit and receive information over the communication network directly, i.e., without using any gateway, (b) devices that communicate information (transmitting and receiving) through gateways, (c) devices that communicate directly without the use of the communication network but being able to communicate over local networks or to form ad hoc networks, and (d) devices that are able to selectively turn on and off functionality in order to save operating power. In regard to gateways, the device layer includes all relevant communication technologies, wired and wireless, such as CAN bus, Wi-Fi, Bluetooth, Zigbee, etc. Importantly, the device layer includes protocol conversion, because devices may implement different protocols, and, thus, needs protocol conversion for interoperability.

The network layer provides encapsulation of device data and related protocol conversion to network layer protocols. The layer includes functionality for the network and transport layers in the OSI protocol reference model. For networking, they include control functionality for network connectivity, mobility, authentication, authorization, and accounting, while for transport they anticipate user traffic transport as well as the transport of control and management information for (I)IoT service and applications.

The service support and application support layer includes both generic and service/application-specific functionality (capabilities) that enable (I)IoT applications and services. Considering the distributed nature of (I)IoT services and applications, there exists generic functionality, such as data processing and storage, as well as specialized functionality, per application and service, since emerging services have different requirements, for example, smart grid operation places different privacy requirements than an intelligent toll management system for transportation services.

Finally, the application layer, the highest hierarchical layer, includes the (I)IoT applications and services.

The management vertical, crosscutting layer includes both generic and application domain-specific functionality. The generic one refers to the typical management for configuration, topology, resource, performance, fault, security, and account management. The application-specific one refers to functions that meet application requirements, such as smart meter monitoring in smart grids.

Analogously to the management layer, the security vertical, crosscutting layer includes both generic and application domain-specific functionality. The generic functionality refers typically to functions related to authorization, authentication, integrity and confidentiality at all layers, privacy at the application layer, secure routing at the network layer, access control at all layers, etc. Application-specific functionality refers to meeting application-specific requirements.

The ITU reference model document presents also a set of business models for IoT, considering the large number of stakeholders in the area and their different interests and goals. Importantly, these business models are developed based on the view of network operators. The business models are based on five main business roles that the stakeholders may have: (a) device provider, (b) network provider, (c) platform provider, (d) application provider, and (e) application customer. As the terms indicate, device providers are the stakeholders that provide devices for (I)IoT, and network providers provide network systems, gateways, and connectivity for the (I)IoT. Platform providers provide the unified, distributed IT platform with well-defined interfaces, over which an application can be served end to end, while application providers are the ones who provide the (I)IoT service over the platform, networks, and devices provided by the corresponding providers. Apparently, the application customer is the user of the (I)IoT application or service.

Based on these five business roles, ITU identifies five business models depending on the number of operators that are involved in an application and their specific roles. Figure 5.4 shows these five models (Models 1–5), presenting the business roles as stacked boxes – analogously to the vertical layer model – and indicating operators with different fill patterns in the boxes; boxes (roles) with the same fill pattern in a stack indicate that the same organization is the operator of these boxes. In Model 1, for example, the same organization has the roles of device, network,

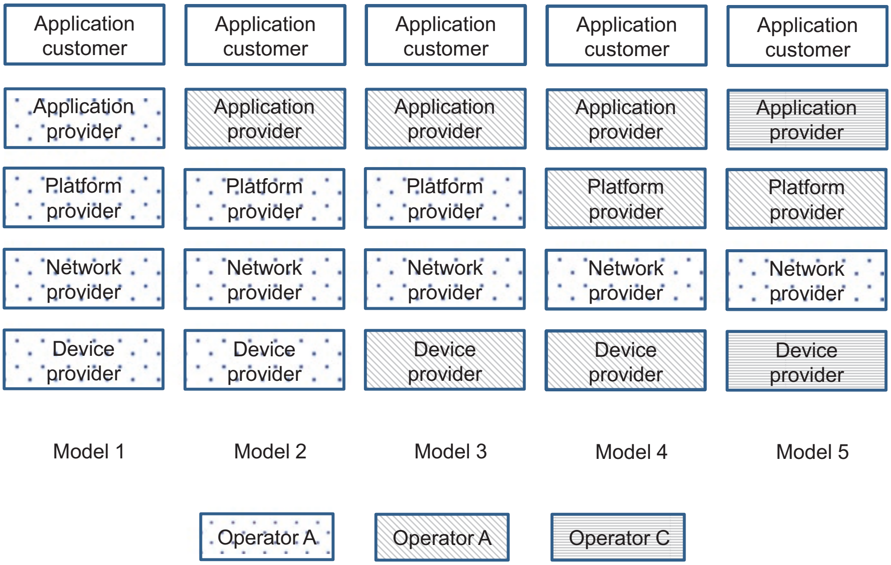


Fig. 5.4 IoT business models identified by ITU

platform, and application provider, while, in Model 2, one stakeholder has the roles of device, network, and platform provider and another one has the role of the application provider.

The Industrial Internet Consortium (IIC) focuses on similar concepts and develops a reference IIoT architecture that has several similarities with the ITU approach and reference model. Clearly, the IIC approach to the architecture development addresses the interests and concerns of all types of stakeholders in an integrated way, originating from use cases and focusing on complete business models and applications at all levels, from devices to IIoT services. IIC follows the approach that different stakeholders who need to make different decisions have architectural viewpoints that are at different levels of abstraction. These viewpoints enable stakeholders to focus on the parameters of interest and develop appropriate architectures that achieve their goals and address the problems they have identified. For this purpose, IIC has identified four different viewpoints: (a) business, (b) usage, (c) functional, and (d) implementation.

The business viewpoint addresses the concerns of business stakeholders, who define and specify IIoT systems and services in their organizations or for customers. These concerns, such as return on investment, cost of maintenance, and similar, are addressed through a model that enables the definition of visions and values which are translated to key objectives and then to high-level specifications of business tasks, named fundamental capabilities. The stakeholders involved include business developers as well as system engineers and product managers.

The usage viewpoint describes how the system is used, implementing the key objectives and the capabilities that have been specified through the business viewpoint. The viewpoint is described with a model that identifies the system and its activities, the involved parties – humans or machines – and their roles, and, finally, tasks, i.e., actions that are executed by parties with a specific role. As tasks are the actions in the system, they are precisely specified and described per role with, so called, functional and implementation maps that specify the exact functions and implementation subsystems that are necessary for a task's complete execution. The stakeholders involved in the usage view include not only the systems engineers and the product managers of the related employed products but all stakeholders that are involved in IIoT system and service specification, including the end users.

The functional viewpoint presents the functional architecture of the IIoT system, describing its components, dependencies, and coordination, meeting the requirements and specifications that have been developed through the usage viewpoint. The stakeholders involved in this viewpoint are system and subsystem developers, product developers, and managers as well as system integrators.

Considering the focus of IIC on IIoT and the increasing adoption of industrial control systems (ICS) within the industries of several sectors and in the operation and management of critical infrastructure, the IIC reference model focuses on its functional architecture of IIoT systems on the integration of ICS with classical information technology (IT) systems in a unified, effective model that meets the requirements of all stakeholders – as specified in the business and usage viewpoints – and enables their effective decisions. The inclusion of ICS and IT in a unified model presents several challenges. Industrial control systems, the systems of Operational Technology (OT), have been developed following a different evolution path from typical IT systems, because of their goals and requirements that typically include continuous operation, safety, and real-time constraints; OT systems have been mostly developed and owned by control and operations engineers, they employ different technologies for processing, communications, and interfaces because they interface directly with the environment through sensors and actuators, and they are managed by their owners independently, since they are typically part of demanding systems and services in terms of dependability, continuous operation, real time, and safety. As a result, their technologies, practices, and standards have evolved independently from the ones for IT. However, the increasing capabilities offered by advanced sensors and actuators, processors, and memories have enabled ICS to execute highly complex operations that have been developed for complex IT systems, such as high-volume data collection and analysis, multivariable modeling and optimization, etc. Importantly, at the same time, the increased capabilities and the increasing complexity of ICS have led them to be more vulnerable to failures and cyber-attacks, leading to additional functional requirements for their correct and efficient operation.

In order to address the integration of IT and OT in a unified model, the IIC approach to the reference architecture divides IIoT systems in five domains, each one grouping the functionality required for a logically distinct high-level operation of the system. These five domains are (a) control, (b) operations, (c) information, (d) application, and (e) business. Figure 5.5, from [IIC17], illustrates the decomposition of the functional representation of an IIoT system into the five domains and

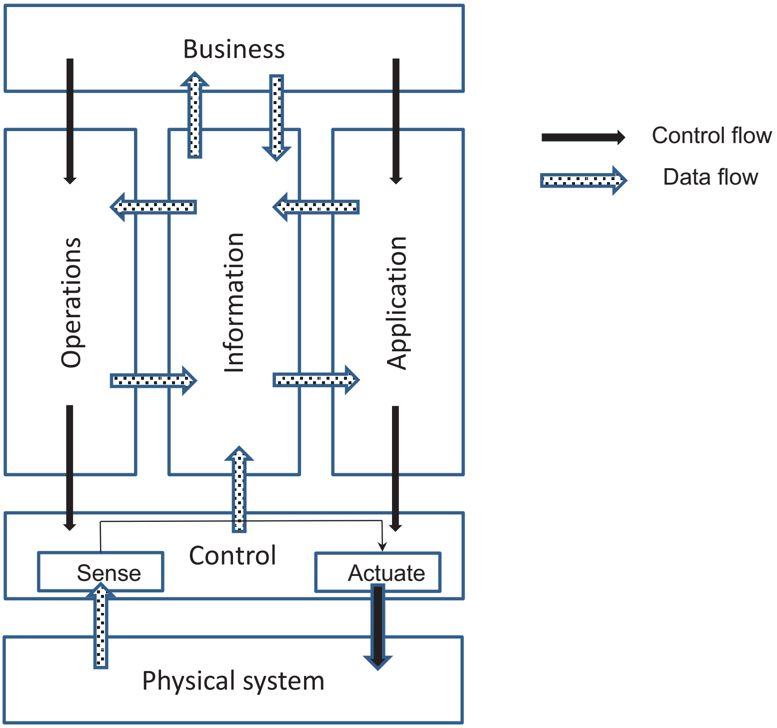


Fig. 5.5 The IIC reference architecture functional domains

shows the data and control flow among the domains, as specified by IIC. The control domain effectively represents the control loop realized by industrial control systems, i.e., it contains the sensors, the logic, and the actuation that constitute a plant implemented by one or more industrial control systems. The operations domain includes the functions that are required for the operation of the industrial control systems in the control domain; the operation includes system monitoring and management as well as optimization for the efficient operation of the systems, especially considering the requirements of several application domains for continuous operation, meeting real-time requirements, and achievement of low-power objectives. The information domain is responsible for collecting data from all domains and analyzing them to enable high-level decisions for the system, e.g., coordinating and optimizing the end-to-end operation of several industrial control systems in the control domain. The application domain includes functionality that is application-dependent and effectively includes the models and operation rules of the application at hand; an important part of this domain is the set of APIs and user interfaces so that other applications or human users can use the application effectively. Finally, the business domain includes systems and functions that enable management and decision making at the business level, e.g., with enterprise resource planning systems (ERP), manufacturing execution systems (MES), etc.

It is important to note that the IIC approach is centered around the concept of a control plant, i.e., it addresses all viewpoints around a control loop that implements a plant. Since control loops can be simple, with one system, or complex with multiple systems typically organized in a hierarchy, the IIC functional domain decomposition can be applied at all levels of a hierarchy. Thus, the decomposition of an IIoT system in the domains does not represent a layered approach as the ITU approach, but rather a logical functional decomposition within a layer or across layers in a hierarchy. Because of this, the IIC reference architecture identifies "crosscutting functions" that are effectively hierarchical (or layered) IT infrastructure functions necessary for the development of a complete IIoT application. These functions include connectivity, distributed data management, analytics, intelligent and resilient control, and any other application function that is necessary for the specific application domain or use case. For example, connectivity has to be implemented in a hierarchical fashion, following standards and practices, interconnecting components within an industrial control system or across several such systems, where each system can be viewed as a collection of functions from all five specified domains. Observing the crosscutting functions mentioned, one can realize that they effectively constitute a layered architecture analogous to the one by ITU. In that respect, one can consider the IIC approach and the ITU approach as complementary, with the IIC reference architecture being a generalization of the ITU one, since it includes crosscutting functions analogous to the ITU layers, while it enables the development of more detailed functional models per layer addressing complete control loops and providing support to all types of stakeholders – from device designers to business developers – for effective decision making.

This analogy and complementarity becomes more apparent with the implementation viewpoint, which addresses the implementation details of the functional viewpoint developed for an IIoT system. The implementation viewpoint includes all the necessary technical and technological details that are necessary for the implementation of a complete IIoT system and its application, including system functionality, technological requirements, communication and network protocols, all types of interfaces, and a mapping of the functional blocks that are specified in the functional viewpoint onto typical implementation architectures, such as the three-tier architecture (where the three tiers are the edge, platform, and enterprise) and the layered databus architecture.

5.5 Basic Technologies

The basic technologies that enable the evolution of IIoT are the sensors, cyber-physical systems, and the related communications and networking technologies that enable their connectivity, among them or to other systems, including enterprise networks. As basic technologies, we designate the ones that are all common to all application domains and use cases.

A fundamental technology for IIoT, and IoT in general, is the technology of RFID (radio-frequency identification) which enables the transmission of a microchip's identification information to a reader over wireless media. It is one of the first technologies that enabled and supported the IoT concept, because RFID technology enabled the automatic identification, monitoring, and operation execution related to RFID-equipped tags. For this reason, RFID technology spread widely since the 1980s in the applications for logistics and supply chain management [Fuq15].

Wireless sensor networks (WSN) constitute another fundamental technology for IIoT, considering their widespread employment in industrial automation and their increasing deployment in critical infrastructures. The solutions for effective WSNs need to address a large number of issues, ranging from communication reliability and real-time requirements to low-power communication due to the deployment of a large number of battery-operated sensors in the field. The significant advances in the area have resulted to a large number of potential solutions and standards for reliable and efficient communication in various environments, e.g., WLAN, Zigbee [Zig], Bluetooth [Blu], 6LoWPAN [Mon07, Hui11, She12], etc. Importantly, they have led to the development of smart (intelligent) sensors, even ones that are autonomous and do not need recharging [Eno].

In addition to the low-level communication protocols that are necessary for connectivity, additional, higher-level protocols are necessary to support distributed computing operations and IIoT applications. Such protocols include service discovery, e.g., multicast DNS (mDNS) [Che13], as well as application protocols that are suitable for the various IIoT application domains such as Constrained Application Protocol (CoAP) [She14], Message Queue Telemetry Transport (MQTT) [Mqt16], and Advanced Message Queuing Protocol (AMQP) [Amq14].

5.6 Applications and Challenges

IIoT applications span a wide range of IoT application domains. Operational technology (OT) systems have become the basic computation platform for the operation and management of most critical infrastructure. The high processing and storage capacity of PLCs, their ability to manage real-time applications with high availability, and their easy management by available SCADA systems have made them quite popular as building blocks of large infrastructures beyond the manufacturing floor, for which they were originally introduced. Today, a large portion of infrastructure is based on industrial control systems (ICS) and makes this critical infrastructure a potential provider of IIoT services and user of IIoT technology. The energy sector is probably the most demanding one on the use of ICS, since the production and processing of energy is part of a country's heavy industry and thus, naturally, includes large ICS platforms. In addition, ICS are used heavily in power distribution networks, such as the electricity network. Considering the emerging smart grids that provide monitoring devices, i.e., PLC-like systems, to customers, it becomes apparent that ICS are the main computing infrastructure in power systems end to end, from production to consumption.

A large number of distribution networks follows this ICS-based model of operation, including water distribution and management networks and water processing sites. Importantly, oil and gas distribution networks use this technology managing pipelines and storage tanks as well as the overall network's operation. Transportation also presents a significant area of application, where ICS and other cyber-physical systems are used for traffic management, i.e., operation and management of traffic lights, for toll payment, etc.

All these application areas of IIoT will require additional deployment and adoption of components, especially cyber-physical and ICS in particular, in order to provide the envisioned services at a large enough scale to improve the lives of citizens significantly. The IIoT revolution is still at its beginning. In this evolution process, the sectors that currently depend on ICS technology will be the forerunners of IIoT technology and will provide the leadership in IIoT development. Currently, the power sector and especially the electricity production, distribution, and consumption processes are the most mature ones, having large bases of ICS at most stages of the service provisioning infrastructure. Despite its maturity, the sector presents quite challenging problems for its next generations. We present some of these challenges here, as a sample illustration of the continuous challenges that need to be resolved in the path to IIoT. Analogous problems exist in other IIoT application areas as well, but the scope of our presentation is to illustrate directions and not to enumerate problems in all application domains.

Stability and continuous operation of the power production and distribution systems constitutes a critical requirement for the development of modern economies. Monitoring the state of the power grid system is a challenging process that is feasible through advanced techniques for fault diagnosis and identification. In this direction and considering the advances in smart grids, we need more advanced techniques for fault detection and isolation in environments with distributed, interconnected power generators. Detection methods based on $\chi 2$ distribution statistics enable one to identify, with a high degree of confidence, whether the grid operates well or if there is a fault; furthermore, fault localization and isolation can be achieved by applying such techniques in segments of the grid. Conventional methods for distributed fault diagnosis are limited though, because they do not address the nonlinear dynamics of the grid's behavior, using either algebraic methods that do not address the dynamics or sets of linear differential equations that do not address the nonlinear characteristics. Currently, there is significant effort to develop methods for distributed fault diagnosis taking into account the nonlinear dynamics, focusing on nonlinear modeling, nonlinear state estimation, nonparametric state estimation, development for statistical criteria for fault diagnosis and isolation as well as observability, and diagnosis with distributed sensor networks in the power grid [Rig11, Rig13, Rig15, Rig17].

Power optimization of large consumers, such as large organizations or buildings like hospitals, etc., is a significant challenge which can be addressed by IIoT. Data collection and preparation for processing are critical to the implementation of innovative power management and control. Actually, data preparation is emerging as a critical, time-consuming process especially in heterogeneous environments, requiring the adoption of new and innovative methods for data cleaning, accounting, grouping, and conversion, so that data are presented to processing in a homogeneous fashion. A promising direction to the optimization of power consumption is the identification of patterns in consumption, based on the collected data. Pattern recognition methods play an important role here in two directions, specifically recognition of patterns based on real consumer behavior and development of desired patterns that lead to lower consumptions [Kok09, Hat11, Kou11].

Installation of IoT technologies at a large scale, as in the case of buildings, energy networks, and production lines, requires appropriate processes, mechanisms, and tools. The tools for deployment and configuration for the IoT, and especially IIoT, subsystems constitute a challenge because of the high complexity and heterogeneity of the cyber-physical systems used [Ant16]. The problem becomes more acute when considering the limited resources of wireless embedded systems, the strict requirements for initialization of secure wireless connections, and the requirements for monitoring the parameters that are used for scheduling in real-time wireless networks, such as IEEE 802.15.4e, IETF 6TiSCH6top, and ISA 100.11a [Kou16]. In contrast with small-scale deployments, e.g., in home environments, installation processes at a large scale are error prone, despite their formalization, and lead to installations that have significant costs for reinstallation or reconfiguration when new devices are added or when changes are made, e.g., an office floor reconfiguration. A characteristic example of a formalized, but error-prone, installation method is the "outside-in" installation sequence, where sensors, actuators, and controllers can be installed by technicians before the network, and IT infrastructure in the building is installed. Clearly, it is necessary to develop effective tools for the management of IIoT resources such as wireless sensors and their networks.

IoT technologies, in general, are easily adopted in the industrial and enterprise environments [Bi14], while the addition of wireless cards for the identification of products and materials enables the management of their complete life cycle [CEP10]. Thus, there is a need to integrate these smart and identifiable objects in the industrial enterprise infrastructure and processes. Considering the heterogeneity that characterizes industrial enterprise environments and its layered management, from high-level ERP systems to low-level production management systems, the integration of these devices achieving interoperability is a clear challenge. However, when the challenge is met, the resulting system enables the flexibility of industrial processes and their mapping and distribution on "things" of the IIoT, increasing autonomy within the enterprise.

References

[Amq14] ISO/IEC 19464:2014 (2014). Information technology: Advanced message queuing protocol (AMQP) v1.0 specification.

[Ant16] Antonopoulos, C., et al. (2016). Integrated toolset for WSN application planning development commissioning and maintenance: The WSN-DPCM ARTEMIS-JU Project. *MDPI Sensors*.

[Bi14] Bi, Z., Xu, L. D., & Wang, C. (2014). Internet of Things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics, 10*(2), 1537–1546.

[Blu] Bluetooth specifications. https://www.bluetooth.com/

[CEP10] (2010, March). CERP-IoT vision and challenges for realising the Internet of Things. CERP-IoT – Cluster of European research projects on the Internet of Things.

[Che13] Chesire, S., & Krochmal, M. (2013). Multicast DNS. *IETF RFC, 6762*.

[Eno] EnOcean Alliance. https://www.enocean-alliance.org

[FoF] Factories of the Future. European factories of the Future Research Association (EFFRA). http://ec.europa.eu/research/industrial_technologies/factories-of-thefuture_en.html

[Fuq15] Al- Fuqaha, A., et al. (2015). Internet of things: A survey on enabling technologies protocols and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.

[GE17] GE Digital. Industrial Internet insights from GE Digital. https://www.ge.com/digital/content/industrial-insights-from-ge-digital

[Hat11] Hatziargyriou, N. (2011, September 13–15). Network of the future. *Presentation on behalf of CIGRE TC at the panel session "The electric power system of the future: an international overview". CIGRE international symposium, "The electric power system of the future: Integrating supergrids and microgrids"*. Bologna, Italy.

[Hui11] Hui, J., & Thubert, P. (2011, September). Compression format for IPv6 datagrams over IEEE 802.15.4-based networks. IETF RFC 6282.

[IEC16] OSI. Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO/IEC 27000:2016. http://ww.iso.org

[IIC14] Industrial Internet Consortium. http://www.iiconsortium.org/

[IIC17] IIC. (2017). The industrial Internet of Things volume G1: Reference architecture. IIC:PUB:G1:V1.80:20170131.

[Ind14] Germany Trade and Invest. (2014, July). Industrie 4.0 smart manufacturing for the future.

[ISA16] ISA. (2016, December). The 62443 series of standards – Industrial automation and control systems security. ISA. http://www.isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf

[ITU12] ITU-T. Overview of the Internet of Things. ITU-T SERIES Y: Global information infrastructure Internet protocol aspects and next-generation networks, recommendation Y.20606/2012.

[Kok09] Kok, K., et al. (2009, June 8–11). Smart houses for a smart grid. *20th international conference and exhibition on electricity distribution: Part 1, CIRED 2009*, Prague.

[Kou11] Kourtis, G., Hadjipaschalis, I., & Poullikkas, A. (2011). An overview of load demand and price forecasting methodologies. *International Journal of Energy and Environment, 2*, 123–150.

[Kou16] Koulamas, C., Giannoulis, S., Fournaris, A. (2016). IoT components for secure smart building environments. *Components and services for IoT platforms: Paving the way for IoT standards*. Springer.

[Man13] Manyika, J., et al. (2013, May). Disruptive technologies: Advances that will transform life business and the global economy. McKinsey Global Institute www.mckinsey.com/mgi

[Mic17] Tanner, P. (2017, June 28). Micron benefits from memory market's faster growth rate. Market Realist. http://marketrealist.com/2017/06/micron-benefits-from-memory-markets-faster-growth-rate/

[Mon07] Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007, September). Transmission of IPv6 packets over IEEE 802.15.4 networks. IETF RFC 4944.

[Mqt16] ISO/IEC 20922:2016 Information technology: Message queuing telemetry transport (MQTT) v3.1.1

[Rig11] Rigatos, G. G. (2011). *Modelling and control for intelligent industrial systems: Adaptive algorithms in robotics and industrial engineering*. Springer.

[Rig13] Rigatos, G. (2013). *Advanced models of neural networks: Nonlinear dynamics and stochasticity in biological neurons*. Springer.

[Rig15] Rigatos, G. (2015). *Nonlinear control and filtering using differential flatness approaches: Applications to electromechanical systems*. Springer.

[Rig17] Rigatos, G. (2017). *Intelligent renewable energy systems: Modelling and control*. Springer.

[She12] Shelby, Z., Chakrabarti, S., Nordmark, E., & Bormann, C. (2012, February). Neighbor discovery optimization for IPv6 over low-power wireless personal area networks (6LoWPANs). IETF RFC 6775.

[She14] Shelby, Z., Hartke, K., & Bormann, C. (2014, June). The constrained application protocol (CoAP). IETF RFC 7252.

[Zue10] Zuehlke, D. (2010). SmartFactory—Towards a factory-of-things. *Annual Reviews in Control, 34*(1), 129–138.

[Zig] ZigBee specifications. http://www.zigbee.org/