The Industrial Internet of Things
Networking Framework

An Industrial Internet Consortium Foundational Document

Version – 2021-07-19

David Lou (Huawei), Jan Höller (Ericsson), Dhruvin Patel (Ericsson),
Ulrich Graf (Huawei), Matthew Gillmore (Itron).

CONTENTS

FIGURES

TABLES

The Internet of Things (IoT) fuses the digital realm with the real-world of objects and places and enables digital twins of them. These technologies drive innovation in application areas such as manufacturing, utilities, transportation, logistics and smart cities. The adoption of IoT technologies in industrial settings, known as Industrial Internet of Things (IIoT), enables gathering and analysis of data across machines, physical assets and processes to improve the flexibility and efficiency of systems at reduced cost. IIoT will increase the productivity, shift economies, innovate business models and foster industrial growth: a digital transformation (DX).

The foundation of any IIoT solution is the network that enables the exchange of data and control commands—a system of technologies at the Internet Protocol (IP) and lower layers, and related capabilities such as management and security. Hyper-connectivity underpins digital transformation across industries, [IIC-DX].

Adoption of IIoT applications across a range of industrial sectors are plentiful, and requirements from various perspectives such as business, usage, deployment and performance are diverse. Likewise, existing and emerging networking technologies such as FieldBuses, Time Sensitive Networking, 4G/5G and various other radio technologies target different industrial networking scenarios and applications.[1]

As a result, many options and concerns need to be considered when selecting the right technologies and developing viable and performant network solutions. Wide adoption also demands that solutions are interoperable and hence based on standardized and well-recognized technologies that can be used across industry sectors.

The purpose of this technical document *Industrial Internet of Things Networking Framework* (IINF) is to guide appropriate networking solutions that enable IIoT applications and stimulate industrial transformation. In short, this document provides guidance in answering the fundamental question:

How do I design, deploy and operate a successful
networking solution for my Industrial IoT applications?

[1] *https://www.iiconsortium.org/pdf/Industrial_Networking_Enabling_IIoT_Communication_2018_08_29.pdf*

1 CONTEXT

1.1 SCOPE

The *Industrial Internet of Things Networking Framework* supplements the *Industrial Internet of Things Reference Architecture* (IIRA) and *Industrial Internet of Things Connectivity Framework* (IICF) by detailing the requirements, technologies, standards and solutions for networking supporting diverse applications and deployments across a broad range of IIoT sectors and vertical industries. Knowledge of IIRA [IIC-IIRA] and IICF [IIC-IICF] is not a prerequisite for using this report.

The IINF has its foundation in the IIRA [IIC-IIRA] defining viewpoints, industrial sectors and lifecycle processes, see Figure 1-1. It is elaborated and contextualized to IIoT networking below.

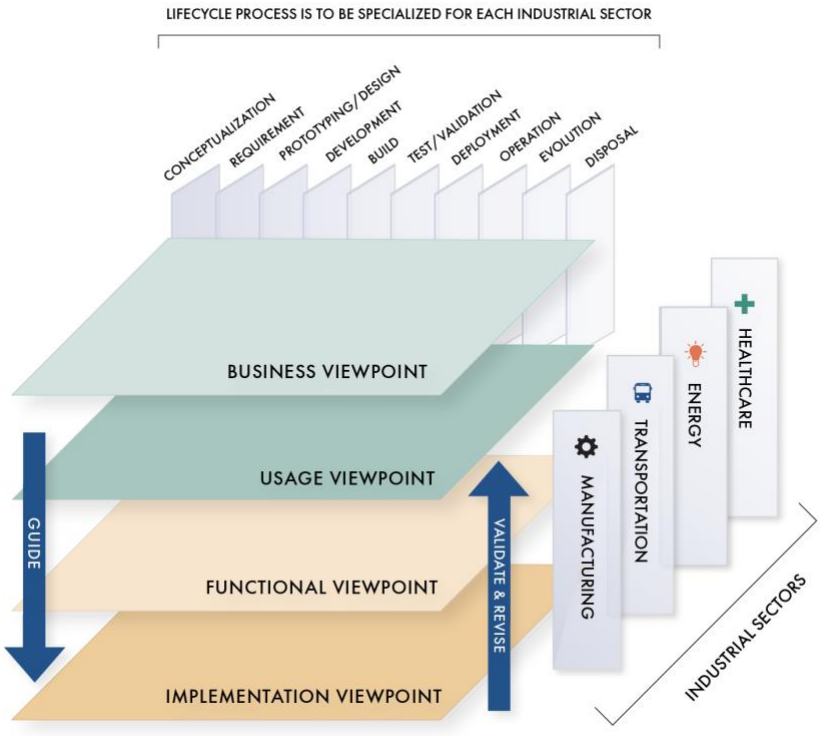

Figure 1-1: IIRA Architecture Framework

The IIRA defines a set of cross-cutting functions that need to be supported across several functional domains of an IIoT system. One of those cross-cutting functions is the *communication* cross-cutting function, see Figure 1-2. From a functional perspective, the communication cross-cutting function enables exchange of information between endpoints in an IIoT system and the physical systems of devices and controllers attached to operational technology (OT) equipment.

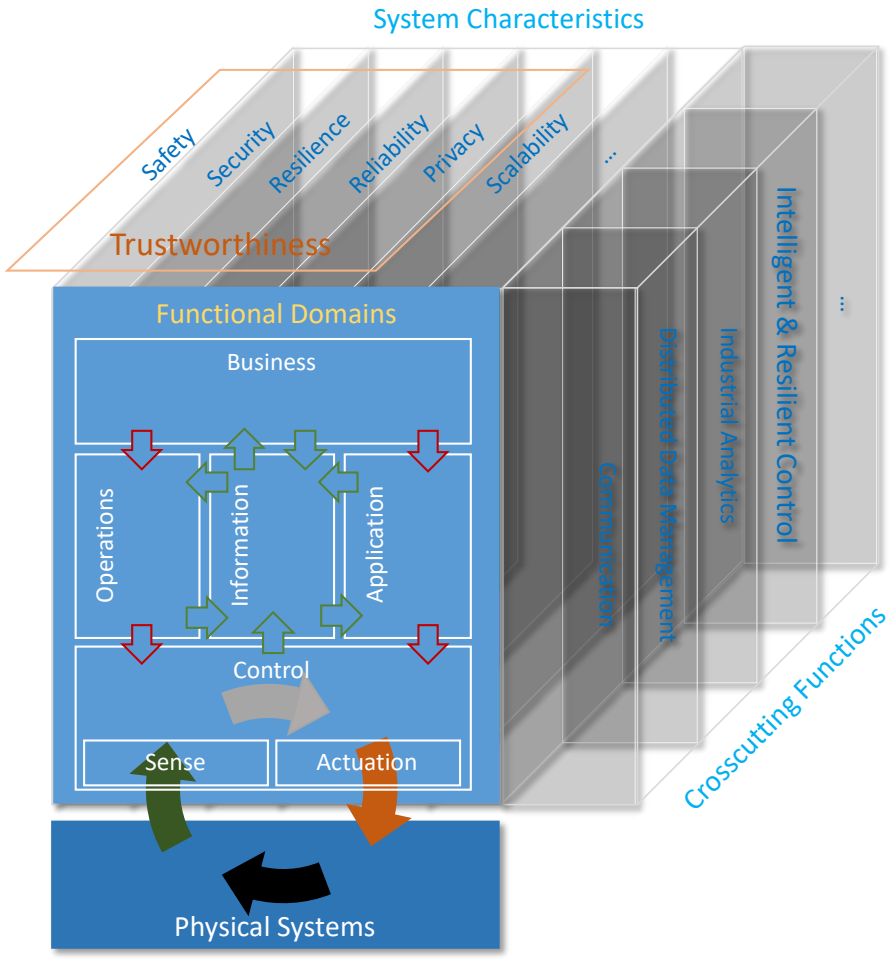

Figure 1-2: Cross-cutting functions, system characteristics and functional domains of IIRA including data and information flows

More precisely, the general role of communication is to exchange information, which includes:

- the transparent transmission of bit streams on a physical medium,
- the transfer of data units over network segments and networks,
- message exchanges carrying data units between endpoints,
- the proper data encoding (syntax) and
- information meaning (semantics), see [IIC-DDIM].

Networking is a sub-function of the communication cross-cutting function as shown in Figure 1-3. It covers transmission of data over a medium and the transfer of data units over a network.

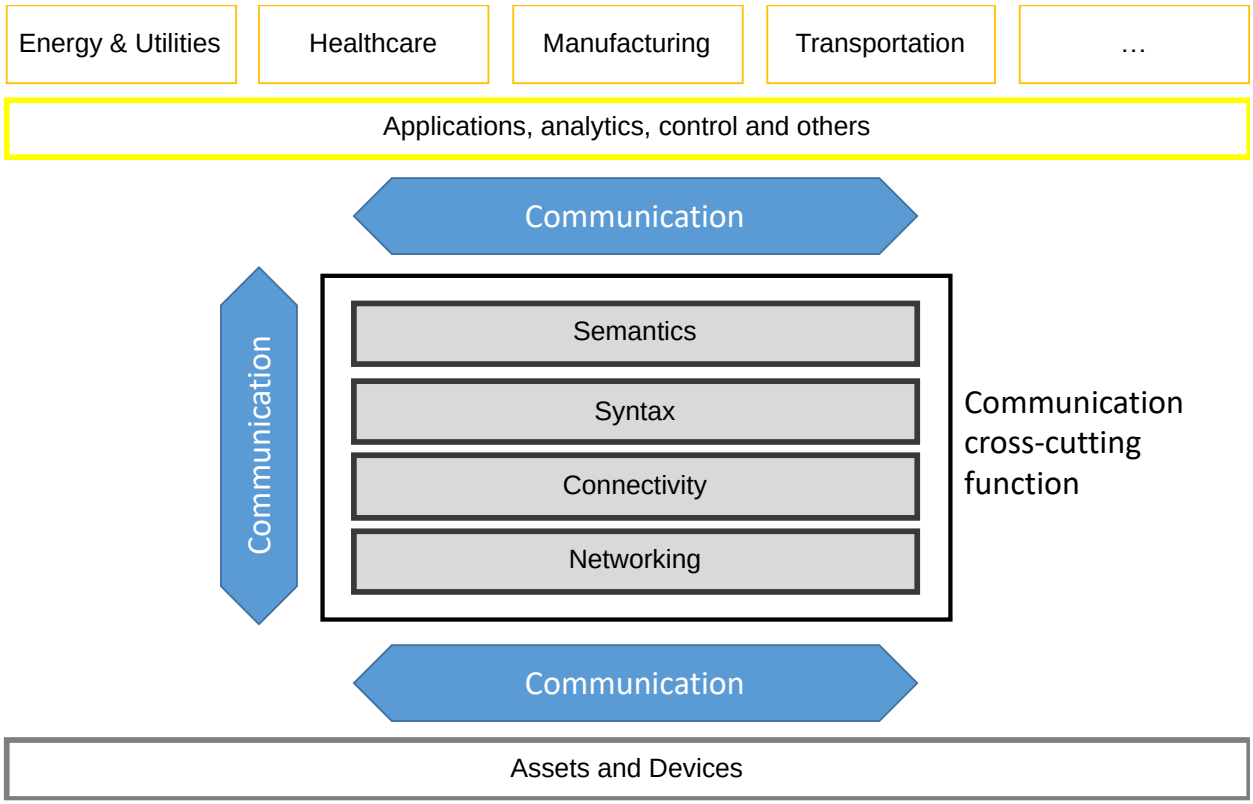

Figure 1-3: Networking as part of the Communication cross-cutting function

The definition, and hence the scope, of networking in the context of IIC is based on the lower three layers of the Open Systems Interconnection (OSI) reference model [ISO/IEC 7498], i.e. OSI layers 1, 2 and 3, which are the Physical, the Data Link and the Network Layers, respectively. This corresponds to the Networking, Link and Internet Layers of the Internet Model, see [IETF-RFC1122].

This IINF covers stakeholders and their concerns pertinent to networking across the four IIRA viewpoints (Business, Usage, Functional, Implementation), and lifecycle process perspectives. Technology-oriented concerns covering the Functional and Implementation viewpoints are further refined as requirements. Example use cases from several industrial sectors are provided as illustrations of the diversity of considerations in networking. Further, functional architecture views and networking architecture patterns are summarized. Networking technologies and standards are covered, including their assessments related to concerns and technical requirements. Finally, architecture blueprints are provided as networking best practices.

1.2 RELATION TO OTHER ARCHITECTURE VIEWS AND IIC PUBLICATIONS

The IINF and its model supports and is supported by other elements of the IIC portfolio including:

The *Industrial Internet Security Framework* (IISF) [IIC-IISF]: Security of networks is imperative. The IISF describes the four building blocks of communication and connectivity protection: network

configuration and management, network monitoring and analysis, communicating endpoint protection and physical security of connections. These building blocks and other key networking elements of the IISF can be considered as an additional set of concerns for the IINF model.

The *Industrial Internet Connectivity Framework* (IICF) [IIC-IICF]: The IICF and the IINF are inherently linked by the common relationship to the OSI and Internet models. The IINF focuses on the lower three layers and the IICF on the upper layers of the models. The shared boundary of these two frameworks is the network layer, highlighted in the IINF as the internet protocol layer and described in IICF as follows: *"The Internet Protocol (IP) is the prevailing network layer connectivity standard that has given birth to the Internet and now IIoT. The IP network layer has enabled independent innovation, both below and above the network layer. The physical, link, and network layers have been in use longer; although evolution of IP and non-IP connections and the multitude of wireless-access technologies coming to market create new choices for the IIoT community."*

IIC testbeds: A central element of IIoT is a network. IIC testbeds[1] address a diverse range of applications demonstrating solutions to use cases in many different industrial sectors. The testbeds both inform and are informed by the concerns and requirements of the IINF model.

1.3 WHAT YOU GET FROM THIS REPORT

This document serves as a guideline and toolbox for any IIoT networking solution stakeholder, whether focusing on design, development, deployment or operation. As such, the intended audience of this document includes system architects, business architects, network solution architects, product managers, production managers, network operators, system engineers, technology evaluators and technology decision makers.

We address needs from business and technical architects and others to create a concrete network solution tailored for the requirements and concerns for a specific industrial application. It can be used as a reference for a deeper dive into networking technologies and standards. It identifies interests from stakeholders and defines requirements to consider. It introduces networking technologies and how to assess them given a set of requirements to narrow down the set of choices. Specifically, it addresses the following questions:

- Who are the main stakeholders that should care about networking solutions and what should be their main concerns?
- What are possible business and operational models for networking?
- What are examples of networking scenarios from different industry segments that can assist in identifying possible networking solutions?
- What are the business and usage criteria to consider when designing a networking solution and evaluating possible networking technologies?

[1] *https://www.iiconsortium.org/test-beds.htm*

- What are the relevant technical requirements to consider when assessing a technology?
- What are relevant available and emerging technologies, and how do they fulfill different expectations and requirements?
- What are networking architecture patterns that solve typical problems?
- What are best practice examples of typical network solutions for different industry sectors?

2 FRAMEWORK OVERVIEW AND VIEWPOINTS

2.1 APPROACH

Finding a networking solution starts with identifying the different *viewpoints* of relevance, the relevant *stakeholders* and their *concerns*. IIRA has defined four viewpoints, each of which identifies a set of stakeholders. The stakeholders have different interests that can be expressed as concerns and then as requirements. This applies to the different parts of an IIoT system, and its lifecycles. The main lifecycle stages include design, development, deployment and operations of IIoT networks, which could also encompass re-design, extension and decommissioning.

The IINF breaks down the problem at hand using IIRA viewpoints and a set of framework tools and methods depicted in Figure 2-1, which are covered in a subsequent chapter. The starting point is to identify the stakeholders and their main concerns, develop and understand business and usage needs for an industrial scenario, drilling down through requirements and finally, to solution and technology scoping and concrete recommendations.

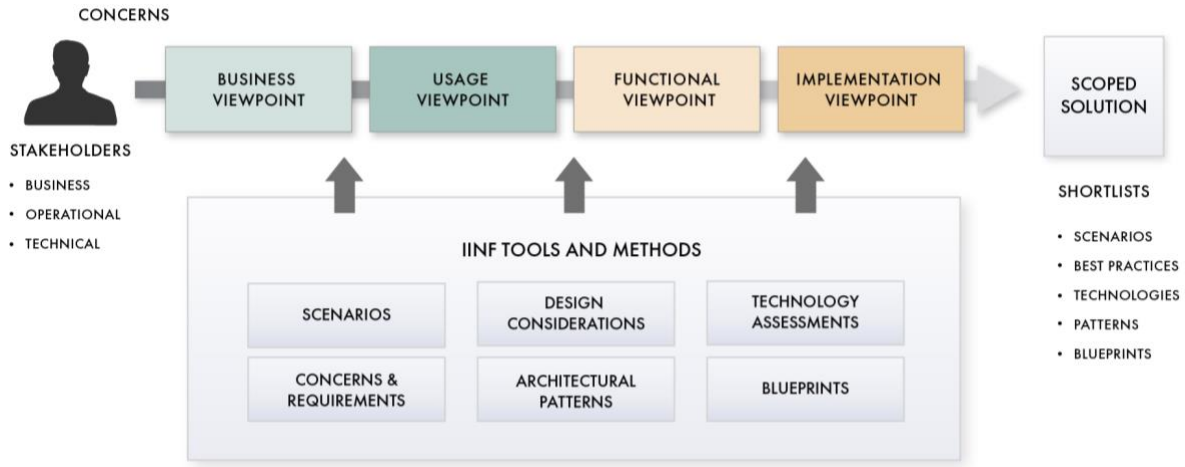

Figure 2-1: The IINF approach based on the IIRA viewpoints

The IINF tools and methods provide the framework for understanding of the target solution and the selection of appropriate technologies. The result of applying each tool or method adds details on the definition of requirements or on recommended elements of a solution. Employing a

particular tool or method provides a partial deliverable of understanding and knowledge, which can also be used as input to an adjacent tool or method. The following sections employ this serial structure by explaining inputs, procedures and outputs of the individual tools and methods from the left (input) to the right (output), from the business vision to the implementation. These tools and methods serve the following purposes:

The *business viewpoint formulation* derives actionable key objectives (measurable through KPIs) and fundamental (system) capabilities from a business vision.

The *usage viewpoint formulation* delivers an understanding of applications, operational aspects and activities to achieve the desired fundamental capabilities. This covers the expected system usage and represents the intended functionality at a high level.

The outputs of the business and usage viewpoints constitute an industrial scenario, which we call an *industrial networking scenario*. Formulations of the business models and the use cases cannot be limited to networking; the functional and implementation viewpoints can take the portions into account that are relevant to the lower three layers of the communications stack. The relevant understanding leading towards an IIoT networking solution is articulated by considering a set of *business concerns* and *usage concerns*.

The functional and implementation viewpoints are technology oriented, and for the sake of simplicity, they are collapsed into a technical viewpoint below. Most of the IINF assets are associated with the functional and implementation viewpoints, and are specified as:

Networking *concerns* and *requirements* are captured for the defined industrial scenario. The concerns are defined at an intermediary level of complexity and cover fairly broad aspects, and a subset of the concerns are further refined as requirements. Network requirements refer to functional or non-functional technical parameters, the latter often include quantitative statements. The network requirements are independent from technologies and available implementations. The definition of requirements serves two purposes: as a tool to extract specific requirements pertaining to the industrial scenario of interest, and as a tool to assess available and emerging networking technologies and their applicability to the industrial scenario.

The scenario is an input to *design considerations* that provide additional context, such as environmental aspects, often qualitatively. They may also account for previous implementations.

System design often relies on a set of *architecture patterns* that are recurring practices of successful solution examples, and they are here covered as *network architecture patterns*.

Network implementations rely on a selection of a set of available and standardized technologies, and provide an understanding of suitable choices, *technology assessments* are provided to help map the requirements into technology recommendations.

Finally, *blueprints* are provided that illustrate best-practice networking solution examples for different industrial networking scenarios.

The outcome of applying the IINF assets and processes is a scoped solution description characterized by detailed scenarios, key stakeholder concerns and requirements, identified and assessed technologies suitable for meeting the identified requirements across the viewpoints, any appropriate architecture patterns and example best-practice blueprints. The IINF, then:

- facilitates the extraction and capture of stakeholder concerns and requirements,
- provides the tools to assess properties and capabilities of different networking technologies on par level and
- provides guidance in the selection of technologies and solution approaches.

The relevant networking stakeholders and groups of concerns are summarized in Figure 2-2. It is based on the viewpoints (with "technical" combining the functional and implementation viewpoints) and covers the main lifecycle stages.

VIEWPOINTS	BUSINESS	USAGE	TECHNICAL
STAKEHOLDERS	• BUSINESS ARCHITECT • COO, CFO, CSO	• PRODUCT MANAGER • OT OPERATIONS • NETWORK OPERATIONS	• NETWORK SOLUTIONS ARCHITECT • SYSTEMS ENGINEER
CONCERNS	• BUSINESS MODEL • TOTAL COST OF OWNERSHIP • REGULATORY • TECHNOLOGY GOVERNANCE	• DEVELOPMENT CONTEXTS • LIFECYCLE PERSPECTIVES • OPERATIONAL PERSPECTIVES • APPLICATIONS	• TRAFFIC CHARACTERISTICS • DEPENDABILITY • MOBILITY • COVERAGE & REACH • E2E NETWORKING • SECURITY

Figure 2-2: Summary of stakeholders and concerns

2.2 BUSINESS VIEWPOINT

The *business viewpoint* attends to the concerns of the identification of stakeholders and their business vision, values and objectives in establishing an IIoT system in its business and regulatory contexts. It identifies how the IIoT system achieves the stated objectives through its mapping to fundamental system capabilities. For a more in-depth discussion on business strategy considerations in IIoT, refer to the IIC Business Strategy and Innovation Framework.[1]

Business-oriented concerns such as business objectives, business value, choice of business model, expected return on investment, cost of ownership, and liability must be evaluated when considering an IIoT system as a solution for overall business objectives. The business viewpoint

[1] *https://www.iiconsortium.org/BSIF.htm*

helps business architects align and maintain their IoT business capabilities in respect to networking needs. For the best practices and processes that IIoT practitioners need to implement IIoT strategy and execute IIoT projects, see the Resource Hub.[1]

A fundamental question is the business objectives for adopting IIoT. Is it to transform internal processes, such as optimization of resource usage, increased productivity, shorten time to market or increased quality, or is it to find new means to deliver products or services to reinvent business delivery or tap into new revenue streams? As businesses explore IIoT, they often transform their products into as-a-service business models. The underlying networking technology can directly affect a new products-as-a-service business. For instance, network availability, reliability and coverage range affects service continuity as IIoT products move in and out of the coverage area or the network is not available when needed. Another example is how power consumption, data rate and transaction rate influence design of products or vice versa.

Some businesses may deploy out-of-the-box network connectivity embedded into the products using public mobile networks or network-as-a-service over a global IoT network, or over reliable private 4G/5G networks to free them from the restrictions around mobility of Ethernet or Wi-Fi networks. Others may choose unlicensed network connectivity such as Wi-Fi relying on the end users' responsibilities for its availability and configuration. Depending on the network connectivity types and business models, the cost of network connectivity can be free, paid separately by the end users or embedded into the price of the connected products and services.

Stakeholders include business architects, CxOs (financial, strategy, operations, marketing) and roles with procurement and partnering responsibilities.

The business viewpoint has the following main categories of concerns including considerations as concrete questions detailing the overall business concerns:

Business model: What are the overall business objectives? Are you selling an IoT-enabled product, using IoT in your internal processes, or to digitalize external processes across a value network? Networking can be provided by own installations, or can be outsourced to third parties, such as Carriage Service Providers or other Network Service Providers (NSPs). Networking can also be a combination: own installations at a site and via service providers between sites. Considerations such as service-level agreements (SLAs) then become relevant. Will networking be embedded into a product and service offering or an explicit add-on, and if the former, what effect do networking costs have on the overall business case? If networking is needed across involved partners in a value chain, what are the principles for taking or sharing costs? What are your target or key customers and partners? Business model concerns also cover go-to-market considerations, such as pricing models and time to market.

[1] *https://www.iiconsortium.org/wc-bse.htm*

Total cost of ownership includes costs related to networking from different lifecycle perspectives and include both CAPEX and OPEX. CAPEX examples include cost for chipsets and technology licensing, while the latter is related to technology governance. OPEX includes the cost for using a networking service, typically either operating own installations, or relying on third-party suppliers of networking services. What are budget considerations in both fixed and variable costs?

Regulatory aspects relate to use of wireless licensed or unlicensed spectrum, safety and electromagnetic fields (EMF) and choices of wireless vs. wireline, and what wireless technology to use. Different wireless technologies can also use different frequency bands depending on country or region. Licensed spectrum can require the engagement of public NSPs, but can also, on a national or regional level, be available for enterprises, or can be used as shared spectrum. For any international operations, national regulations must be consulted. Safety regulations typically relate to EMF health and can have regulations specific to industry segments.

Technology governance deals with both how standards are governed, i.e. whether they are openly standardized, developed in closed member groups or *de facto*, and how general or specific they are, in particular understanding the implications from relying on industry domain-specific standards compared to generally applicable and available technologies. The costs of licensing and the longevity of a particular technology depend on who provides technology: a single supplier or an established ecosystem of suppliers.

2.3 USAGE VIEWPOINT

The *usage viewpoint* addresses expected system usage. It is typically represented as sequences of activities involving human, system or system-components users that deliver its functionality. Usage-related concerns serve as input for deriving system requirements that guide the design, implementation, deployment, operations and evolution of the IIoT system over the lifecycle. The stakeholders here are system engineers, product managers and specifiers of the system, operators and the ultimate users of solutions and applications realized by the system.

Stakeholders: The usage viewpoint captures concerns from operations managers and specialists across OT, IT and networks, production managers, to include both OT-related production and production or delivery of network services. Concerns can also come from application developers, quality managers, IT security officers and safety officers. The ultimate users of the applications and services that the IIoT system delivers are those that have interests related to OT operations and OT-related deliveries. Product managers and application-service providers involved in connected products in the field also have usage concerns.

The below categories of usage concerns are used to characterize IIoT networking technologies.

Deployment contexts include considerations of where and at what scale networking is expected, what resources are available to support networking, and under what environmental conditions. Harsh properties such as temperature, humidity, chemical and physical conditions affect the choice of grade of equipment, be it devices, networking equipment or cabling. Those

environmental conditions can also affect whether to use wired or wireless networking. If deployments are in confined spaces, radio propagation or cabling can be issues. From a scale perspective, is networking needed to be only local (site, factory), regional, national, international, or global and what is the number of connected devices? From a wide-area perspective, urban vs. extremely remote (e.g. marine) areas will affect the choice of networking, such as mobile networking or even combined with satellite.

Lifecycle perspectives: Networked devices, networks and their technologies evolve at a different pace from OT. OT deployments are long lived and operational over decades, whereas IT typically evolves over a few years. Detaching these different lifecycles is needed and it requires ease of upgrades to software and firmware, or ease of replacement if related to hardware. Are interfaces in place that support any lifecycle requirements?

Operational perspectives cover the management and operational needs. How are deployments provisioned from a lifecycle perspective, and monitored from a fault and performance perspective, for instance, when networking services are provided by a third party? Some device deployments will be unreachable, requiring full remote-management and operability including firmware upgrades. Will there be need for retrofitting or swapping of devices? Are the deployments brownfield or greenfield? The former requires a strategy for co-existence either separated or integrated. How are devices powered, by battery, energy harvesting or via mains supply?

What *applications* will be supported over the network and what are their service needs? A unified single network approach is desirable, but some applications might have different requirements that justify separate network segments in parallel from both a technical and business viewpoint. What evolution is foreseen for new applications, what is the need for a futureproof network and for what timescale? There are also design considerations covered in section 4.1.

2.4 TECHNICAL VIEWPOINTS

The *functional viewpoint* focuses on the functional components in an IIoT system, their structure and interrelations, the interfaces and interactions between them, and the relation and interactions of the system with external elements in the environment, to support the usages and activities of the overall system. These concerns are of particular interest to system and component architects, developers and integrators.

The *implementation viewpoint* deals with the technologies needed to implement the functional components of the functional viewpoint, their communication schemes and their lifecycle procedures. These elements are coordinated by activities (usage viewpoint) and supportive of the system capabilities (business viewpoint). System and component architects, developers and integrators, and system operators are concerned with these.

Stakeholders: The technical viewpoint is of primary relevance for network solutions architects, network planning engineers, network system integrators, component and subsystem developers, network systems engineers and IT security engineers.

Here, the technical concerns are used both to capture networking requirements and to assess different technologies in the assessment templates. The relevant requirements and their definitions are provided in section 4.2.

Traffic characteristics cover requirements and capabilities like uplink and downlink bit rates, packet sizes, periodicity in communication and traffic capacity per geographical area (bits/area).

Dependability is the measure of the reliability and availability of networking, and to some extent, its security and durability. Reliability for networking is defined by how well data is delivered and preserved. Reliability can be described as guaranteed throughput, bit and packet error rates, latency, jitter or latency variation, both from a link level and end-to-end. Related are terms like deterministic networking (upper bound of latency) vs. more relaxed networking, providing only intermittent connectivity. Availability is how robust a service is, expressed in terms of percentage compared to service outage. Dependability also covers software and hardware robustness and how these technologies are certified.

Mobility relates to devices, where they are deployed and if they are mobile, both spatial mobility, and in reference to networks. Spatial mobility considerations include geographical area and speed, i.e. local/site/sub-site, national or global scale. Mobility is also about what level of networking service continuity is required, as such nomadic use of communication, depends on the network coverage. Nomadism could be relevant when considering infrequent re-configurability of deployments.

Coverage and reach: What area or volume is to be covered and what is the density in terms of devices and traffic per unit? What is the reach in terms of distance, is there line of sight (underground mining vs. open-pit mining) and are there specific propagation conditions such as radio propagation conditions and spectrum efficiency, or what is attenuation and cross talk for wireline solutions?

End-to-end networking addresses resulting traffic characteristics and dependability measures. Are there specific needs for network segmentation due to deployment scenarios, security perimeters, upper layer gateways/intermediaries like proxies or to control SLAs?

Security is primarily about threat protection of deployments and their operations, and about data confidentiality, integrity and privacy. Deployment protection can be solved by dedicated deployments with complete isolation or isolation via de-militarized zones using firewalls and similar measures. The use of open networks or openly available networking technologies require specific consideration of required security. Security for data protection is a combined consideration of devices, networks and applications and can be solved at different layers such as

link and network/IP and transport layers, as well as at the application layer. Depending on the needs, data protection measures at different layers can be required in parallel.

3 INDUSTRIAL IOT SCENARIOS

Industrial internet scenarios and use cases establish the technical and commercial requirements for networks. IIC has identified the following core industries for the industrial internet:

- energy,
- healthcare,
- manufacturing,
- mining,
- retail,
- smart cities and
- transportation.

These industrial domains identified by IIC offer a rich palette from which to extract scenarios that can be analyzed for consistent networking patterns. The objective here is to develop a method, through application of representative examples of scenarios from various industrial domains, to allow the reader to apply their own experience to map needs to patterns.

3.1 MANUFACTURING OF CONSUMER-PACKAGED GOODS (CPG) – PACKAGING LINE

Industrial domain: A packaging line for consumer-packaged goods.

Application scenario: Manufacturers of consumer-packaged goods such as canned food, breakfast cereal, shelf-stable beverages and others rely on specialized machinery to process the product and make it ready for shipping and sale with attractive packaging. The production machinery employs repeatable, yet flexible procedures to deposit the product into its primary packaging and then combine the primary packages into one or more bulk packages (for example, soup cans will be filled with soup at a filling station, the cans will be closed in a second operation and labeled in a third, and loaded into cartons or trays to be loaded onto pallets for storage and shipment).

The speed of the filling and packaging has a direct effect on the productivity of the manufacturing operation. Automated machinery has enabled speeds approaching the mechanical capabilities of the equipment. Product quality and product throughput are very important to the production owners (plant manager, operations manager, line operator and machine operator).

As more automation is applied in packaging operations, operating speeds have increased. Industrial networks have evolved from low-speed serial networks to the high-speed IP-based networks today. As more advanced technology is added, the complexity of applying and maintaining the technology increases. When a machine experiences an unplanned outage, production stops and concerned stakeholders pay attention.

A critical part of machinery operation is the operation of the networks that work within each machine, between each machine and between machines and business systems. Some machine actions are sensitive to timing to ensure precise placement of materials throughout packaging.

Networking technologies: For intra- and inter-machine networking, the following network technologies are prevalent:

- Layer 1 (Physical Layer): IEEE 802.3 Ethernet,
- Layer 2 (Link Layer): IEEE 802.3 Ethernet, IEEE 802.1 including extensions for Time Sensitive Networking (TSN) and
- Layer 3 (Networking Layer): Internet protocol.

Environmental properties: Packaging operations are often in near-ambient environments although some applications require tight control of temperature, humidity and sanitation. In general, manufacturing is a noisy environment due to the number of pieces of rotating equipment and their respective control gear. Because of the products themselves, and the requirement for sanitation, the environment is often subjected to wet and wash-down conditions, which make it important to protect the electronics for the networking equipment.

Scenario/application networking requirements: A summary of networking related requirements is listed in Table 3-1.

Coverage area	Dictated by the size of the manufacturing hall 1 ~ 1000 meters
Speed/communication rate	Basic sensing and actuating: 10 ms Precise synchronization: 1 µs
Capacity	100 Mb to 1 Gb
Reliability	Highly deterministic Security: Average to strong network security
Power	Typically, mains powered; no significant restriction
Commercial	Competitive acquisition cost Low lifecycle cost for maintenance, upgrade

Table 3-1: Networking requirements for packaging line scenario

Testbed reference(s): This scenario can use elements of the IIC *Time Sensitive Networking (TSN) testbed*.

3.2 REMOTELY CONTROLLED MINE

Industrial domain: The mining industrial sector is an important source of raw materials.

Application scenario: The mining industry has improved its productivity, increased worker safety and reduced its environmental impact by using remotely controlled vehicles and machinery. As more automated machinery is deployed, mining companies can explore areas they have not been able to reach safely with humans. More automation and new exploration areas lead to new problems for networks that connect machinery to the operators and the information systems.

A remotely operated machine or highly mobile vehicle could have as many as six to eight high-resolution cameras for simultaneous video feedback, light detection and ranging imaging to provide a 3D perspective, haptic feedback to operators and machine telemetry. A large number of sensors give a distributed view of the ore body and mine environment and the data must be analyzed in near-real-time and with ultra-high reliability requirements.

Traditionally, networking for mining applications was accomplished using a combination of wired (leaky coax) and wireless technologies. Wireless networking used unlicensed spectrum and, in many cases, proprietary technology. As more networking was added to meet the needs of the new vehicles and machinery, miners demanded more standardized approaches to the problem.

Networking technologies: A range of wireline and wireless networking technologies can be found in the modern remotely controlled mine:

- Layer 1 (Physical Layer): wireless and wireline connectivity, such as IEEE 802.3 Ethernet
- Layer 2 (Link Layer): IEEE 802.1 TSN, IEEE 802.11, IEEE 802.15.4 and 3GPP (4G/5G)
- Layer 3 (Networking Layer): Internet protocol

Environmental properties: Mines are inherently dirty and dusty and electromagnetic noise from equipment is prevalent. Underground environments are physically constrained and impenetrable. Open mines expose equipment to weather conditions.

Scenario/application networking requirements: A summary of networking related requirements is listed in Table 3-2.

Coverage area	Dictated by the size or depth of the mine 1000s of meters
Speed/communication rate	Local sensing and actuating: 10 ms Responsive to ergonomic tolerances for haptic feedback
Capacity	100 Mbps per machine or higher
Reliability	Latency: 200ms end-to-end

	Security: Average to strong network security 99.999% uptime
Power	Typically mains powered; no significant restriction
Commercial	Competitive acquisition cost Low lifecycle cost for maintenance, upgrade

Table 3-2: Networking requirements for remotely controlled mine scenario

Testbed reference(s): Currently there is no IIC testbed related to this scenario.

3.3 CONNECTED SHOP-FLOOR WORKER

Industrial domain: A connected shop-floor worker.

Application scenario: Typical examples of human-machine interface (HMI) are membrane switches, rubber keypads and touchscreens. HMIs include tethered and untethered devices for interaction between the worker and production facilities, such as panels attached to a machine or production line, and standard IT devices, such as laptops, tablets, smartphones, smart watches. Augmented-reality (AR) and mixed-reality (MR) interfaces will likely influence HMIs in the future.

In this scenario, shop-floor workers equipped with devices with mobile connectivity perform maintenance or assembly tasks on the factory floor. They may be assisted remotely by an expert. Before performing the task, he or she locates the equipment and obtains necessary guidance and documentation. Equipment is controlled by a mobile control panel with safety functions. Part of the provided information may be safety-related, indicating foreseen hazards related to the task.

The task is not necessarily a routine, well-documented, follow-the-steps task, but may be caused by an unforeseen situation that does not have pre-described actions. The worker may need to improvise and the system must adapt to that. Execution of the task may be urgent.

This application scenario has two main components: mobile control panels and AR equipment. (Their service requirements are described in TS 22.104[1]). This scenario uses those requirements and it necessitates the simultaneous operation of both control panels and AR equipment.

Control panels are mainly used for configuring, monitoring, debugging, controlling and maintaining machines, robots, cranes, moving devices or complete production lines. In addition, (safety) control panels are typically equipped with an emergency stop button that immediately brings the equipment to a safe stationary position, and an enabling device, which allows the

[1] *https://www.3gpp.org/DynaReport/22104.htm*

equipment to be safely operated during testing or maintenance, when other protection mechanisms (such as a safety fences and cages) are deactivated.

Due to the criticality of these safety functions, safety control panels currently mostly have wire-bound connections to the equipment they control. Consequently, there are many such panels for the many production units in a factory. With an ultra-reliable low-latency mobile connectivity, it is possible to connect mobile control panels with safety functions wirelessly. This would lead to higher usability and allow for flexible and easy re-use of panels for controlling different machines.

People will continue to play an important and substantial role in future smart factories and production facilities. However, due to the envisaged high flexibility and versatility of the factories of the future, shop floor workers should be optimally supported in preparing quickly for new tasks and activities and in ensuring smooth operations in an efficient and ergonomic manner.

Networking technologies: Since the connected shop-floor needs connectivity anytime and everywhere, mobility is key. Wireless cellular or non-cellular technologies are needed on licensed or unlicensed spectrum. Real-time requirements are also inherently necessary for the industrial control and to deliver an appropriate experience of human AR/MR interactions.

- Layer 1 (Physical Layer): Wireless
- Layer 2 (Link Layer): IEEE 802.11, IEEE 802.15.4 and 3GPP (4G/5G)
- Layer 3 (Networking Layer): Internet protocol

Environmental properties: In general, a manufacturing shop-floor is a high electrical-noise environment due to the number of pieces of rotating equipment and their respective control gear. Because of the products themselves and the need for sanitation, the environment is often subjected to wet and wash-down conditions. This makes it important to protect the electronics within which the networking equipment resides.

Scenario/application networking requirements: This application scenario has two main components: mobile control panels and AR equipment. Both have specific service requirements described in TS 22.104. This section summarizes networking requirements for them.

A summary of networking related requirements is listed in Table 3-3.

Coverage area	Dependent on where the connected worker can move, which could be the complete facility. Dense number of access points needed. Coverage area 100 ~ 300 m.
Speed/communication rate	High-rate periodic, bi-directional communication for remote control, such as assembly robots and milling machines. Medium-rate periodic, bi-directional communication for remote control, such as mobile cranes, mobile pumps, fixed portal cranes.

	A-periodic data transmission in parallel to remote control.
Capacity	5 ~ 100 Mbps dependent on service needs.
Reliability	Latency and jitter: 5 ~ 30 ms for responsive applications like AR with haptic feedback. Availability, packet loss: 99,9999 to 99,999999%, MTBF 1 ~ 12 month Security: Average to strong network security
Power	Mobile control panels and AR system is typically powered by batteries. Long battery durability is preferred.
Commercial	Costs depend if cellular or non-cellular technology and if licensed or unlicensed spectrum is used.

Table 3-3: Networking requirements for connected shop-floor worker scenario

Testbed reference(s): Currently there is no IIC testbed related to this scenario. A potential fit could be the smart factory web testbed.

3.4 Onshore Oil and Gas Extraction

Industrial domain: The extraction and processing of oil and gas from onshore wells.

Application scenario: The oil & gas industry is looking for new technologies to improve extraction productivity and supply chain integration. Added to this are further cost reductions and better safety. Well and drilling activities have high capital costs, and take place in environments with significant safety and health risks. Industrial IoT solutions can address needs around safety, hazards and incidents, operational efficiency and uptime of machinery, security and theft avoidance, and supply chain logistics of materials. An on- and inter-site network in this scenario would be in addition to any industrial automation network for real-time control of the extraction and production process and would be used for the following primary purposes:

- Management and monitoring of “un-connected” equipment and machinery performance to predict maintenance and repair cycles better, reduce machinery downtime and understand machinery performance.
- Inspection and surveillance using fixed installations of sensors and video cameras and using drones and crawlers.

Typical applications for onshore production include the following (taken from an example in the Permian Basin in West Texas, US):

- visual monitoring of assets, machines and the security of the site itself using high-definition video cameras operating 24/7/365,

- on-demand inspection of site, constructions, machines and infrastructures using drones and different crawlers to eliminate human inspection cost and risk in many times hazardous environments (heat, flame, chemicals) and hard-to-reach places,
- emergency broadcast in case of incidents,
- incident prevention, like the detection of leakages,
- remote monitoring and preventive maintenance of machinery, and
- near real-time and precise localization and tracking of assets.

Networking technologies: The following summarizes the networking needs at a high level.

- Cellular private network (LTE) at an oil pad site to ease deployment and uniformly connect and manage the different devices and hosting the diverse set of applications.
- Wireless networking to connect devices at a specific oil pad as well as to connect across 100s of different oil pads in a geographic wide area oil field of 100s ~ 1000s km^2.
- Wireless microwave backhaul from (segments of) the oil field with high throughput.

Environmental properties: Outdoor environment of wide temperature range and humidity. Water exposure through precipitation and potential wash down. Exposure to petroleum and chemicals.

Scenario/application networking requirements: A summary of networking related requirements is listed in Table 3-4.

Coverage area	Oil pads are geographically distributed and counts in 100s across oil field segments of 100s ~ 1000s km^2
Speed/communication rate	Video monitoring: 2-10 Mbps, 24/7/365, per unit, one unit per oil pad Preventive maintenance: 100 kbps, per unit, 10 units per oil pad/pump (sensors, gateways, crawlers) Drone for inspection: 4+ Mbps, per unit, 2 units per oil pad Incident prevention monitoring: 100 kbps, per unit, 10 units per oil pad Field worker device (tablet): 200kbps, 1 per 10 oil pads
Capacity	See the field above
Reliability	Latency and jitter: Relaxed (monitoring), 10 ms (AGV, drone operation) Availability, packet loss: Relaxed (monitoring), high (incident detection) Security: Average to strong network security

Power	Typically mains powered; no significant restriction
Commercial	Use of private vs offered services, spectrum (licensed/unlicensed)

Table 3-4: Networking requirements for onshore oil and gas extraction scenario

Testbed reference(s): Currently there is no IIC testbed related to this scenario.

3.5 CONSTRUCTION

Industrial domain: Construction is part of the IIC Manufacturing and Smart City Domains.

Application scenario: A construction project usually lasts from months to years. In some cities, there are thousands of new projects every year while twice that number are in progress. Improving construction efficiency could decrease cycle time and improve economic performance.

Construction projects may have the following needs for digital transformation:

- High-precision indoor positioning: Using indoor positioning technology to control the production device for automatic drilling, painting and other operations.
- Video analysis: Using multi-camera acquisition site construction video data to monitor the working status of workers, and to prevent illegal operations and ensure work efficiency.
- Mixed-reality-assisted construction: Using AR/VR to help the construction experts in site remote guidance and assisted construction.
- Three-dimensional structure data acquisition: Testing the building's stability is the need to analyze the overall three-dimensional structure of the building.
- Efficient management of digitized design, factory production, transportation and other processes in the construction process.

To solve these problems, terminal equipment can be deployed at the construction site, which connects to the transmission equipment and communicates with computing nodes at the network edge. As depicted in Figure 3-1, connectivity to these nodes can be realized with a dedicated line or through a base station. Due to the proximity of edge nodes to the construction site and their compute capabilities, relevant applications being executed can receive the expected latency, bandwidth and security guarantees.

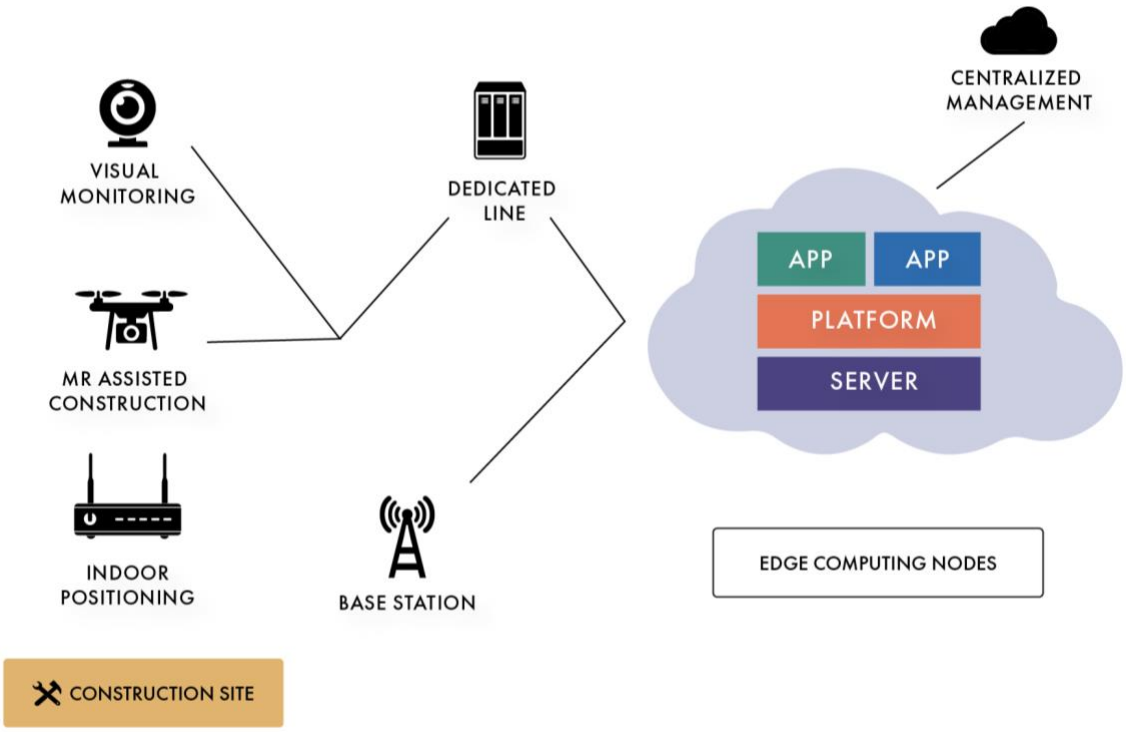

Figure 3-1: Edge computing assisted construction

Networking technologies: A range of networking technologies can be found in the modern construction site:

- Layer 1 (Physical Layer): Ethernet (RS232, RS485 serial interface)
- Layer 2 (Link Layer): Field bus, Industrial Ethernet, Time sensitive network, LTE
- Layer 3 (Network Layer): TCP/IP

Environmental properties: The construction site is generally affected by weather and environmental conditions, and is covered with dust and soil and other adverse conditions.

Scenario/application networking requirements: A summary of networking related requirements is listed in Table 3-5.

Coverage area	Dictated by the size of the construction site 100 ~ 1000s of meters
Speed/communication rate	Local sensing and actuation: 10 ms Responsive to ergonomic tolerances for haptic feedback
Capacity	Up to 1 Gbps per machine
Reliability	Latency: 200ms end-to-end for common application and 30ms for AR/VR

	Security: Average to strong network security 99.999% uptime
Power	Typically mains powered, no significant restriction. Mobile devices powered by batteries.
Commercial	Competitive acquisition cost Low lifecycle cost for maintenance, upgrade

Table 3-5: Networking requirements for construction scenario

Testbed reference(s): Currently there is no IIC testbed related to this scenario.

3.6 SMART GRID

Industrial domain: Smart grids are enhanced with automated control and modern communications technologies to deliver electricity.

Application scenario: Traditional power grids carry power from a few central generators to energy consumers. In contrast, smart grids allow for two-way flows of electricity and information using modern information technologies to deliver power more efficiently and responsively.

Smart grid began with smart meters, which allowed utilities to reduce costs and improve outage restoration by eliminating meter readers and technicians. Today's smart grid infrastructure has enhanced sensing and computing abilities and reliable real-time information flow between all grid components can be implemented only by an advanced communication infrastructure. Utilities are now bringing fiber connectivity to their distribution-level substations and overlaying grid optimization technologies such as sensors and analytics on their field-area networks.

Utilities are ramping up their investments in grid connectivity and networking to improve operating economics, energy efficiency and grid reliability. But there is a growing recognition that the network that supports smart grid applications such as advanced metering infrastructure, distribution automation, and substation automation could become the backbone for far more. The fusion of communications technologies with energy is creating new business models. Utilities intend to build their own private networks for more control and automation and so greater efficiency and reliability. Globally, several trillion dollars will be spent building smart grids by 2030. Another trend is distributed energy resources used and implemented by the traditional energy consumer, therefore balancing demand and supply is another challenge.

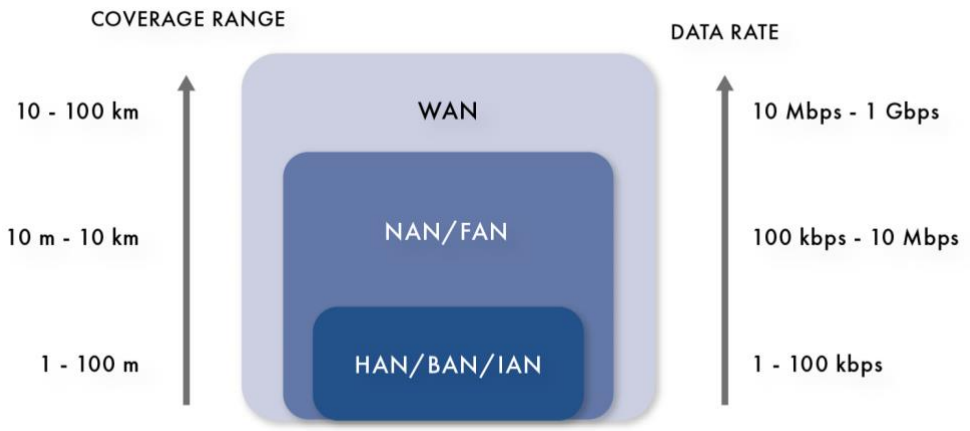

Figure 3-2: Data rate and communication range requirements for smart grid networks

Networking technologies: In a smart grid, the prevalent network and communication technologies include (see **Error! Reference source not found.** above):

- Customer Premises Network (CPN)/Home Area Network (HAN)/Building Area Network (BAN)/Industrial Area Network (IAN)
  - Communication technologies that provide data rate of up to 100 kbps with short coverage distance (up to 100 m) are generally sufficient.
  - Wi-SUN, ZigBee, WiFi, Power Line Carrier (PLC) and Ethernet are widely used to support HAN/ BAN/IAN applications.
- Neighborhood Area Networks (NAN)/Field Area Network (FAN)
  - These applications require communication technologies that support higher data rate (100 kbps–10 Mbps) and larger coverage distance (up to 10 km).
  - Wi-SUN mesh networks, WiFi mesh networks, PLC, as well as long distance wired and wireless technologies, such as WiMAX, 3GPP 3G/4G/5G, Digital Subscriber Line (DSL) and Coaxial Cable support NAN/FAN applications
- Wide Area Network (WAN)
  - This network is extended over thousands of square kilometers and data rates reaches 10 to 100 Mbps.
  - WAN can be implemented using PLC (FSK/BPSK/OFDM), Ethernet networks, WiMAX, 3GPP 3G/4G/5G and Fiber-Optic Communication (SONET/SDH)

To design an efficient and robust network architecture capable of managing operation and control of the next generation power grid, new wired and wireless technologies are emerging.

Environmental properties: Given that smart grids are outdoors, solutions must be capable of operating in line of sight, non-line of sight conditions and operate in temperature extremes of -30º ~ + 60ºC.

Scenario/application networking requirements: A summary of networking related requirements is listed in Table 3-6.

Coverage area	Country-wide coverage, all the way from power generation through transmission, distributed to the energy consumer.
Speed/communication rate	Different for various applications.
Capacity	Large-scale hierarchical network. 100 kbps locally, 10 Mbps regionally and 1 Gbps in wide-area domain.
Reliability	High quality of service (QoS) for the communication and networking technology in all of the stages of the smart grid must be guaranteed. Emergency response and control command should be reliably delivered within required time frame. Latency: Dependent on application up to several seconds. The communication infrastructure needs to ensure exceptionally tight latency characteristics. Security: Average to strong network security 99.999% uptime
Power	Typically mains powered; no significant restriction
Commercial	Competitive acquisition cost Low lifecycle cost for maintenance, upgrade

Table 3-6: Networking requirements for smart grid scenario

Testbed reference(s): This scenario is related to the IIC *Distributed Energy Resources testbed*.

4 CONSIDERATIONS AND REQUIREMENTS

4.1 DESIGN CONSIDERATIONS

The industrial internet is the integration of complex physical production machinery with networked sensors and software. The maturing of the industrial internet and the rapid connectivity of devices to internal networks and the internet are creating significant opportunities for manufacturers that require continuous improvements on reliability, security, deterministic transmission and management capabilities. The design considerations of the IINF to these requirements are described below and an overview is depicted in Figure 4-1.

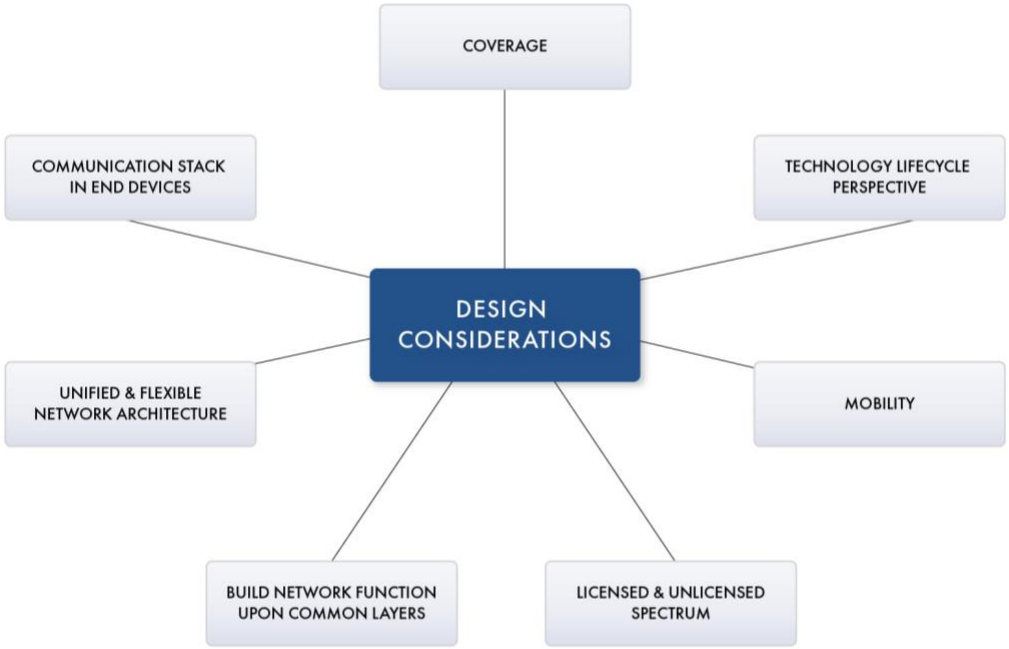

Figure 4-1: Overview of IIoT design considerations

Unified and flexible architecture: Verticals may have versatile scenarios and heterogeneous network requirements. For instance, reliable low latency communication is a key enabler for manufacturing systems, while smart metering in smart cities has different requirements, including low power consumption and long-range communication. Even within one industry, there could be various scenarios requiring different network capabilities. For example, building automation demands soft real-time communication with a cycle time of up to one second, while motion-control communication requires hard real-time transmission with the cycle time being in the range of microseconds. Despite their different requirements, these sectors must be able to communicate. Hence, a common network architecture with ubiquitous connectivity that connects sensor to data centers, interoperates between vendors and spans industries is a key design consideration for IIoT. The network infrastructure, protocols and technologies applied to the industrial internet must be transparent to industrial applications and services to avoid frequent adaptation across various scenarios and verticals. Furthermore, modern assembly lines should be flexible to manage the required product variability without introducing waste or compromising quality. These factors introduce distinctive challenges to existing industrial internet networking technologies. The network should be able to self (re-)configure dynamically to enable the required flexibility in the manufacturing system.

Technology lifecycle perspective: Network technology evolution has consistently followed a cycle similar to Moore's Law with frequent turnover of products and increases in performance. In contrast, OT systems comprise systems with longer life cycles, on average 19 years. This difference in development speed leads to slow adoption of new network technologies into

existing OT deployments. Manufacturing subsystems should therefore be decoupled from the network devices while keeping a consistent interface between them.

Build network function upon common layers: The design principle of the existing internet architecture is built around a common layer. The industrial internet still needs a common layer to incorporate forwarding, switching, control and management capabilities, and to realize additional interoperability, forward compatibility and IT/OT interworking requirements.

Communication stack in end devices: To guarantee reliable, secure and deterministic communication, sophisticated network methods, functions and protocols are required. In the existing industrial network systems, end devices, such as controllers, drives and I/O modules, need considerable resources to realize deterministic transmission. For instance, a manufacturing device must be equipped with a heavy communication stack, or even dedicated hardware to realize hard real-time communication in motion-control scenarios. Although the complexity is manageable in a controller or industrial PCs, it cannot be easily supported by compact drives, sensors or I/O modules. The design of the communication stack and the physical layer hardware of the future industrial network systems should account for the limitations of end devices (resources and power). Therefore the network, rather than the end device, should guarantee that the communication requirements are met.

Licensed and unlicensed spectrum: Due to reliability, coverage and regulatory tradeoffs, the effect of using licensed or unlicensed spectrum must be considered when designing industrial applications with wireless communication.

Coverage: This includes the area to be covered, the number of communication endpoints that need to be supported and bandwidth requirements. Range and reach should include planning for required distances, line of sight and radio propagation properties in the targeted environment.

Mobility: Different levels of mobility define whether support is needed on a global, regional or local level. Local can imply the site or sub-site level. Characteristics of mobility include how frequently mobility occurs, how fast the mobile object is moving and requirements on the bandwidth and latency while mobile.

4.2 REQUIREMENTS

This section presents requirements for the selection of relevant industrial network technologies.

Reliability: According to [ITU-R M.2410] on the requirements for IMT-2020, reliability is defined as the success probability of transmitting a layer 3 packet from source to destination.

Coverage: A technology can have global, national, regional, local (outdoor) and local (indoor) coverage, depending upon its technical characteristics.

Latency: Latency is the time taken for a packet to go from source to destination. Depending upon the use case, the latency requirement can range from milliseconds to seconds. The

communication medium, and whether it is shared or dedicated, plays an important role in determining latency and performance.

Here, basic on the application requirements, we can classify different industrial networking technology into non-real-time (beyond 100 milliseconds), real-time (between 1-100 milliseconds), and extreme real-time (below 1ms).

Peak data rate is the maximum achievable data rate under ideal conditions.

Power consumption rate is the rate of energy drain of a device and is mainly dependent on the choice of networking technology and the communication pattern required from its supported application, e.g. how often a device needs to wake up and communicate. It is a relevant consideration for situations where a device needs to operate without an external power supply and e.g. need to operate on an internal battery. Depending on the deployment situation and the accessibility of operations staff etc, required self-sustained power consumption can be characterized in days, months or years.

Mode of operation: Wireless technology deployment and performance depends upon the type of the spectrum it operates. Radio spectrum can be further classified into licensed spectrum, which requires special authorization from national regulators and license-exempt spectrum that does not. Multiple institutions and companies can share spectrum.

Regulation exists at multiple levels to operate a communication technology.

Redundancy is the duplication of nodes and links in the end-to-end networking between source to destination, which results in high availability and high reliability performance. Few industrial networking technologies inherently support redundancy.

Mobility is the ability of the end devices to communicate independent of their location.

Data security should support data confidentiality, integrity and authentication.

Deterministic behavior is required for an industrial control system. Parameter sensing and relevant machine control needs to be performed within a predefined time period.

*Time synchronizatio*n is a key requirement for a number of use cases related to industrial control, for example, different industrial robots coordinating on the same welding station, distributed measurements gathering on the same scale.

Connection density is the total number of end devices that can be connected per unit area using a given industrial network technology.

5 IIoT Network Architecture

5.1 Networking Overview

5.1.1 The Networking Stack

The seven-layer Open Systems Interconnect (OSI) model and the four-layer TCP/IP model have been widely accepted as conceptual internet communication models; the latter gave birth to the internet and now industrial internet. The bottom three layers of the model, shown in Figure 5-1, (i.e. physical layer, link layer and internetworking layer), experienced rapid evolution over the last decades. For instance, the evolution of IP and non-IP connections, the emergence of new communication protocols and the multitude of wireless-access technologies coming to market create new choices for the IIoT community. The newly introduced protocols, technologies and methods are not widely recognized or understood. This chapter aims to provide a conceptual and functional view of the bottom layers by illustrating their core functionalities and capabilities.

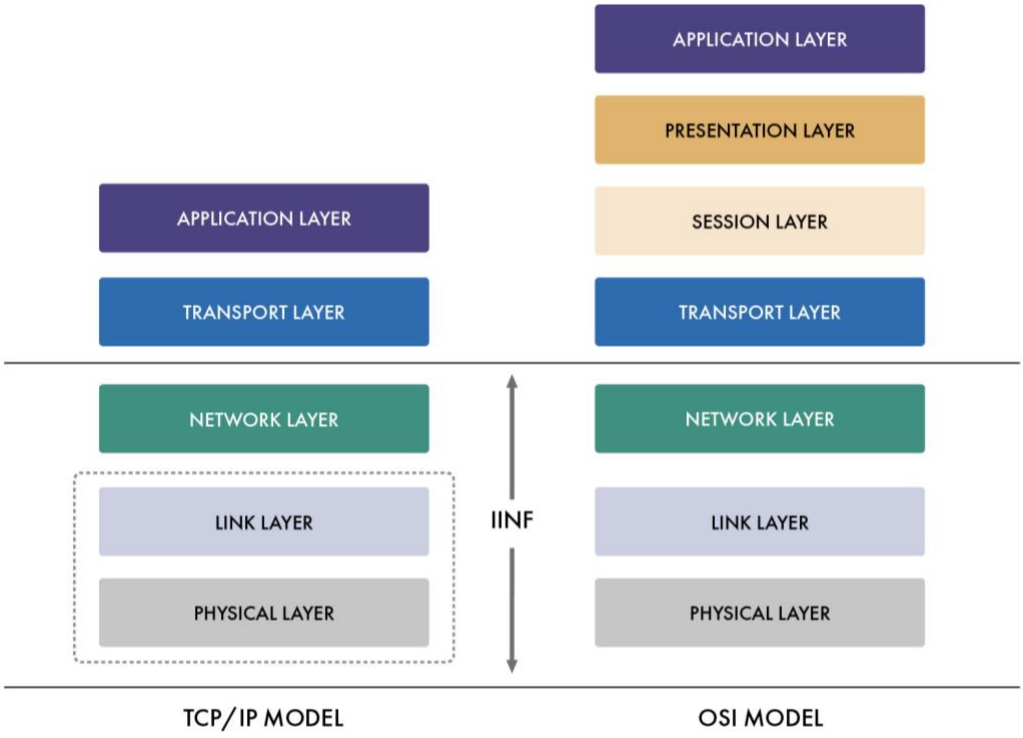

Figure 5-1: The industrial internet communication stack model

The *internetworking layer* (i.e. IP layer) provides the means of transferring data from source entities to destination entities via one or more networks. The internetworking layer responds to service requests from the upper layer and issues service requests to the data link layer. The ultimate goal of the future industrial Internet is a technical integration of systems across domains, hierarchy of IIoT system layers, geographic boundaries, value chains and life cycle phases to connect every step of the industrial process. That means industrial networks may be

within and across a wide area network, which asks for more scalable and deterministic internetworking layer technologies.

Core functions: Traditionally, there are three core internetworking layer functions including addressing, routing and forwarding.

- *Addressing:* Every entity in the network must have a unique address that determines where it is. This address is normally assigned to reflect a hierarchy of the network. IP is the prevailing internetworking layer standard for the internet, which serves two principal functions: host or network interface identification and location addressing.
- *Routing* calculates a path for packets. The routing process usually directs forwarding using routing tables, which maintain a record of the routes to various network destinations.
- *Forwarding:* Packet forwarding relays packets from one network segment to another by network devices in a network. There are three forwarding models in the network: unicasting, broadcasting and multicasting.

The *data link layer* provides the functional and procedural means to transfer data between network entities and can provide the means to detect and possibly correct errors that may occur in the physical layer.

The data link layer is used for delivery of data in the same LAN. It focuses on data addressing, framing, reliability, media arbitration and QoS in the local network. The common data-link data unit is a frame, which does not cross the boundary of a local network.

The data link layer performs simple switching procedures such as MAC address lookup, frame scheduling and shaping, and thus can achieve lower latency and jitter in a local network.

On top of core functions like framing, physical addressing and error control, as shown in Figure 5-2, the data link layer provides capabilities (e.g. scheduling, bandwidth reservation, shaping, etc.) to support quality of service.

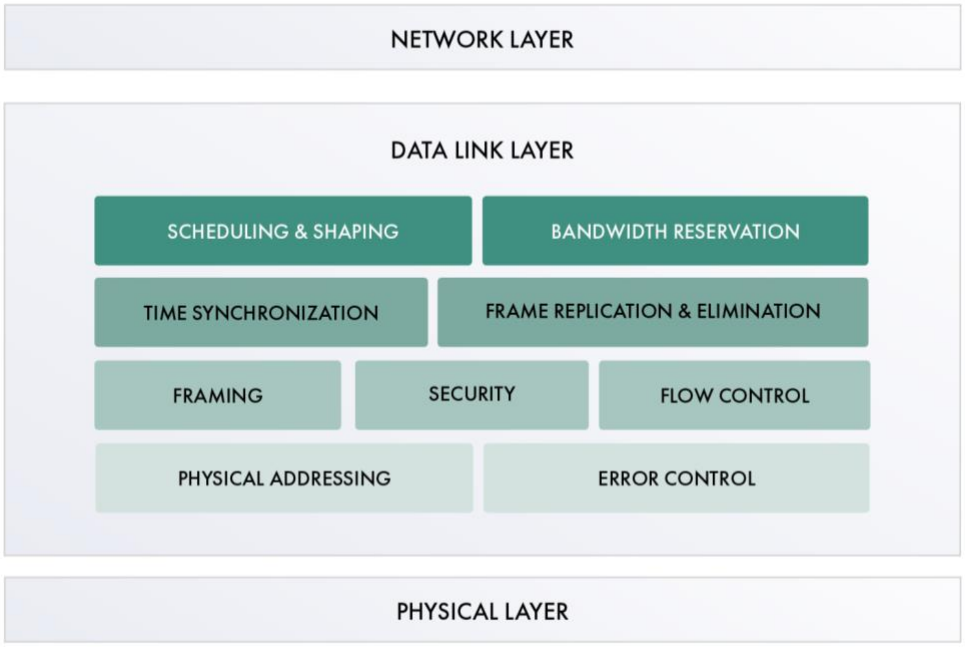

Figure 5-2: Core function at data link layer

- *Framing:* In the data link layer, frames are the manageable data units composed of streams of bits from the network layer. The division of streams of bits is done by the data link layer. In this order, a typical Ethernet frame contains the preamble, the Start Frame Delimiter, the source and destination MAC addresses, the EtherType field, the payload and the Frame Check Sequence.
- *Physical addressing:* The Layer 2 network node can find an output port by the physical address (MAC) of the receiver. Physical addresses must be unique in the local network where the device is located.
- *Error control:* The data link layer provides error notifications that alert higher-layer protocols that an error has occurred on the physical link. The errors include the loss of a signal, the loss of a clocking signal across serial connections and the bit error of a link.

The *physical layer* provides the mechanical, electrical, functional and procedural means to activate, maintain and de-activate physical-connections over a medium for bit transmission between data-link-entities. The key role of the physical layer is to provide physical media (wired or wireless) connections among the endpoints.

The key physical layer functions include encoding and decoding, sequencing (serializing and de-serializing), bit-block multiplexing and de-multiplexing, media multiplexing and de-multiplexing, fault detect and notification, link-status detecting and maintenance, as illustrated in Figure 5-3.

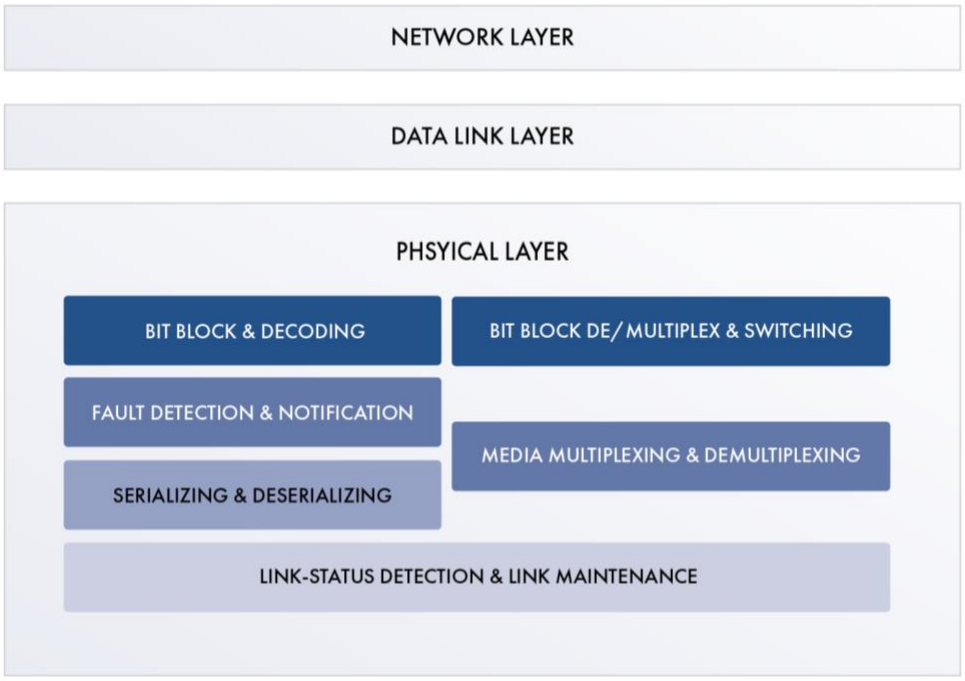

Figure 5-3: Core functions at physical layer

- *Serializing and de-serializing* serializes the encoded bit blocks and transfers the bit stream to the upper layer at the transmission direction.
- *Fault detection and notification* detects fault conditions within encoded bit-blocks of the physical layer and notifies data-link-entities.
- *Link-status monitor and link maintenance* monitors the status of the data-circuit and activates or deactivates physical links.

5.2 NETWORK TOPOLOGIES

An industrial network is made up of programmable logic controllers, human-machine interfaces, computers and I/O devices linked together by communication links such as electric cables, optic fibers, radio links and interface elements such as network cards and gateways. The physical layout of a network is the hardware topology or network architecture. The network topology should adapt to the diverse requirements of an industrial scenario. The most common topologies are bus, star, line and ring, as shown in Figure 5-4.

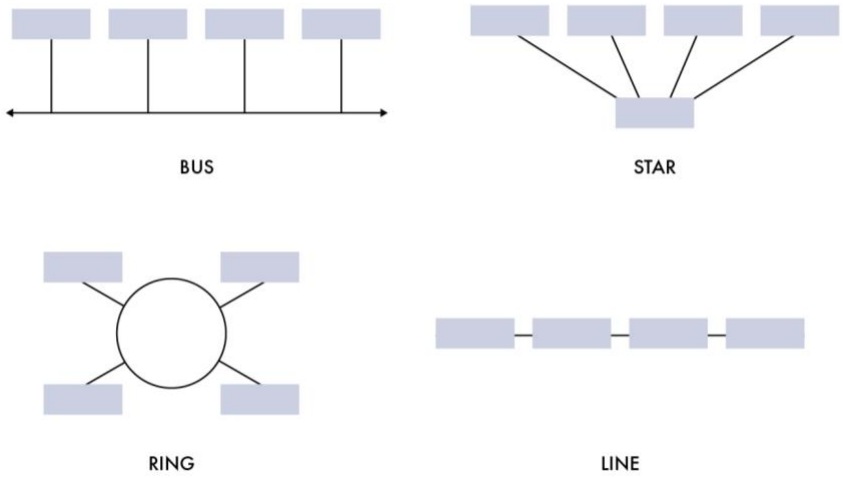

Figure 5-4: Example of topologies in industrial network

Bus topology: This is a simple layout; all the elements are wired together along the same transmission line. The word 'bus' refers to the physical line. This topology is easily implemented, and the failure of a node does not prevent the other devices from communicating. Machine and sensor level networks, otherwise known as field buses, use this system. The bus topology is implemented by linking devices together in a chain or to the main cable via a connection box.

In a *star topology,* end devices are connected and communicate with each other via a home run to a switch. A star network is easy to cable and there is a direct path between the switch and each device. Adding and removing devices does not affect the rest of the network. The major disadvantages are that more cable is required, there is a potential single point of failure with the switch and there is no media redundancy.

In the *line topology*, devices communicate with each other via switches that are daisy-chained together. One advantage of a line over a star network topology is the ability to cover long distances. Another advantage is the simple installation with reduced wiring and installation costs. The primary disadvantages are that any break of the cable or a switch failure will disconnect all devices downstream from the rest of the network, each link in the chain represents network delay and the added expense of multiple switches.

A *ring topology* is similar to the line topology in that each switch is daisy-chained together, but the last switch is connected back to the first to complete the ring. When there is a failure, the switches will detect the failure and still be able to communicate with all of the devices on the network. It would basically act like a network with a line topology until the failure is repaired. The ring topology has a fast recovery time and is easily expandable. The primary disadvantage of the ring topology is the additional setup required to configure each switch.

Dynamic topology: In tomorrow's industries, structures will not be predefined. Instead, a set of IT configuration rules will be defined that can be used case-by-case to build a topology

automatically for every situation. It should adapt to dynamic changes of network topology and provide an ad hoc connecting capability for any nodes at any time.

6 NETWORKING TECHNOLOGIES AND STANDARDS

6.1 OVERVIEW OF THE STANDARDS LANDSCAPE

Today, a wide range of the industrial networking technologies exist to support the diverse set of use cases and requirements. As shown in Figure 6-1, the networking technologies for the bottom three layers in the stack fall in two main groups, namely wireline and wireless; layer three technologies apply to both groups. In wireless, one can generalize the technologies in four main subcategories: Mobile Communication, Low Power Wide Area Network (LPWAN), Short Range Radio and Satellite Communication. In wireline, there are four subcategories: Ethernet, Fieldbus, Power Line Communication and Optical Transport Network.

The most active industrial networking players comes from the data link layer and the physical layer. There are many industrial consortia like PROFINET International (PI), Open DeviceNet Vendors Association (ODVA), Ethernet POWERLINK Standard Group (EPSG), EtherCAT Technology Group (ETG), working on proprietary industrial ethernet technologies, which have been standardized in International Electrotechnical Commission (IEC 61158).

Meanwhile, IEEE, especially IEEE 802.1/802.3, is working on Time-Sensitive Networking (TSN) and IEEE 802.1.5.4 short-range wireless technologies to be applied in the factory. The 3rd Generation Partnership Project (3GPP) focuses on bringing long-range wireless technologies to the industry. The Internet Engineering Task Force (IETF) is one of the major active SDO players in layer three (internetworking layer). In addition, the European Telecommunications Standards Institute (ETSI) aims to also promote innovation on the internetworking layer.

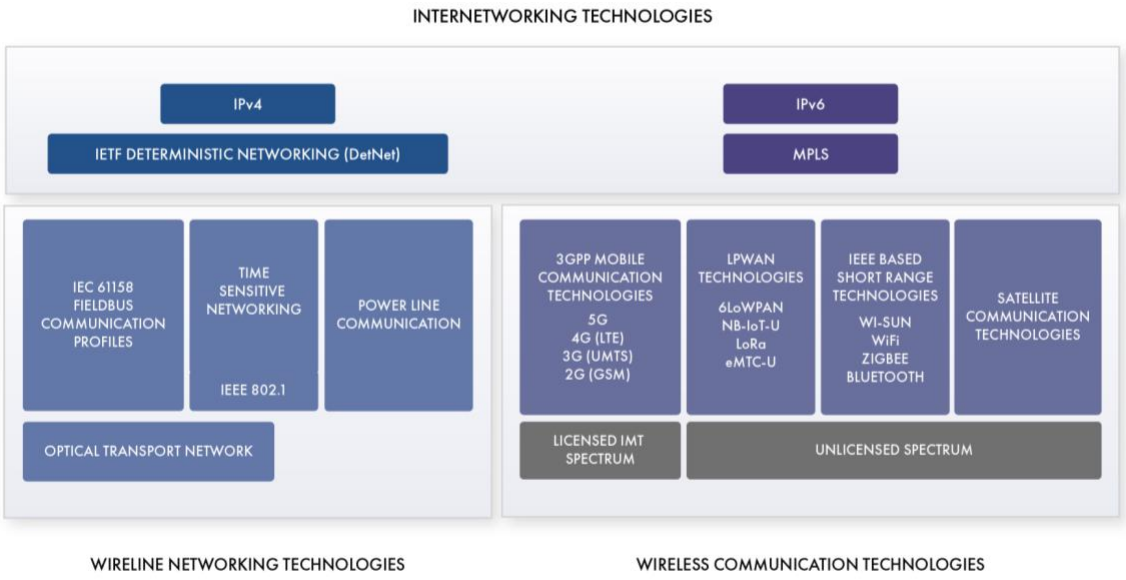

Figure 6-1: A protocol stack-oriented view of the industrial networking standards

6.2 STANDARDS FOR L1 AND L2

6.2.1 3GPP MOBILE TELECOMMUNICATION TECHNOLOGY

The 3rd Generation Partnership Project [1] (3GPP) is the main global standardization body developing the specifications for the cellular and mobile industry communication technologies. 3GPP is an open and global ecosystem driving the development of interoperable standards for mobile and wireless communication technologies. There are around 8 billion mobile broadband subscriptions, the majority being 4G/LTE and 5G increasing significantly, and IoT around 2 billion.[2]

ITU-R is a regulatory body that defines a process for turning 3GPP specifications into global standards. Traditionally 3GPP technologies operate in the licensed parts of the radio spectrum provided by national regulators to mobile network service providers. This license includes rules to manage radio interference, frequency band rights and spectral and geographic dimensions.

The 5th generation mobile communication technology (5G) is the latest mobile communication standard, which is currently evolving to support new use cases. A 5G system comprises new radio access technology called 5G New Radio (NR) in addition include 4G/LTE radio standards, as well as a new core network (5GC) to support a wide range of use cases. The core network is developed based on the principle of the Service Based Architecture (SBA). Figure 6-2 shows 5G system application areas that are categorized in three major communication services, according to the International Mobile Telecommunications (IMT) for 2020 and beyond [ITU-R M.2083]:

[1] *https://www.3gpp.org/*
[2] *https://www.ericsson.com/en/mobility-report*

- eMBB (enhanced Mobile Broadband) enables large data volume and higher end-user data rates than LTE, with enhanced user experience,
- mMTC (massive Machine Type Communication) includes support for the massive number of devices along with lower device costs, significantly lower energy consumption and wider reach and coverage and
- URLLC (Ultra Reliable Low Latency Communication) are for applications that require extreme low latency and ultra-high reliability typically in industrial settings.

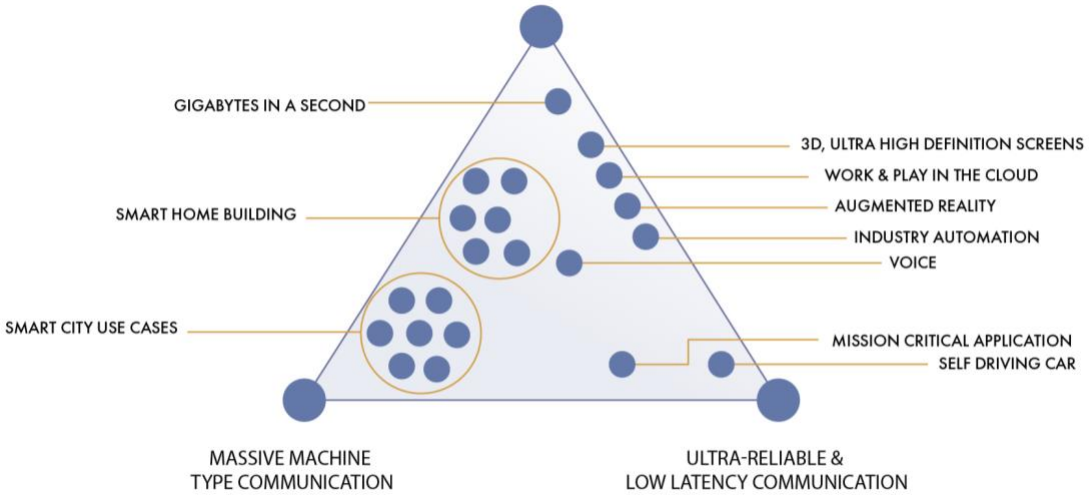

Figure 6-2: 5G application areas (based on ITU-R Recommendation M.2083 [ITU-R M.2083])

To realize such services, a wide range of the 5G technology features have been developed and specified by 3GPP. Some of the important features are:

- URLLC enabled by short transmission slots over air interface enabling fast uplink and downlink transmission,
- mMTC is supported already by NB-IoT (Narrowband IoT) and LTE-M (eMTC) based on 4G,
- high data rates in 5G, enabled by support of NR wide system bandwidth (up to 400MHz), high modulation rates, and massive MIMO antenna technologies,
- 5G Quality of Service (QoS) framework for the traffic flows with diverse communication requirements and
- network slicing to enable multiple isolated virtual networks and features like URLLC, eMBB and mMTC over the same physical network.

3GPP technologies can provide global mobility support and global coverage. The main features and applications of these 3GPP technologies are summarized in Table 6-1, see [3GPP-TR37.910] for specific details.

	NB-IoT	Cat-M1	LTE	5G NR
Peak data rate	˜100 Kbps	1Mbps	25 Gbps (downlink) 12.9 Gbps (uplink)	37.0˜38.6 Gbps (Downlink) 17.9˜18.9 Gbps (uplink)
Reach/coverage	164 dB for 800 MHz band	160 dB for 800 MHz band	144 dB for 800 MHz	-
Latency	<10s	<10s	< 1ms	< 1ms
Reliability	N/A	N/A	N/A	> 99.999%[1]
Battery Life	AA 10 years	10 years	N/A	N/A
Typical apps	Track&trace, env. monitoring	Track&trace env. monitoring	MTC, voice, mMTC	Critical MTC, AR/VR, eMBB
Connection density	>10000000	>10000000	N/A	N/A

Table 6-1: Summary of characteristics and example applications for 3GPP in IIoT

3GPP standardization has further specified support for seamless integration[2] of a 5G System with Time-Sensitive Networking (TSN) networks for industrial communications in-line with the IEEE 802.1 TSN specifications (cf. 6.2.3). Both 5G and TSN have been designed to provide converged connectivity for a range of applications including those requiring deterministic, reliable and low latency connectivity.

This integration enables bridging of TSN networking over 5G as shown in Figure 6-3 where a 5G System is modelled as a virtual TSN bridge. The seamless 5G-TSN integration provides a holistic networking communication solution vertically across field devices and programmable logic controllers (PLC) at a machine or industrial process cell level, via a process or production site level into an enterprise cloud environment. It also provides a solution for horizontal networking across field devices and collaborative machines as part of an industrial process flow.

[1] IMT-2000 requirement

[2] *https://www.5g-acia.org/publications/integration-of-5g-with-time-sensitive-networking-for-industrial-communications/*

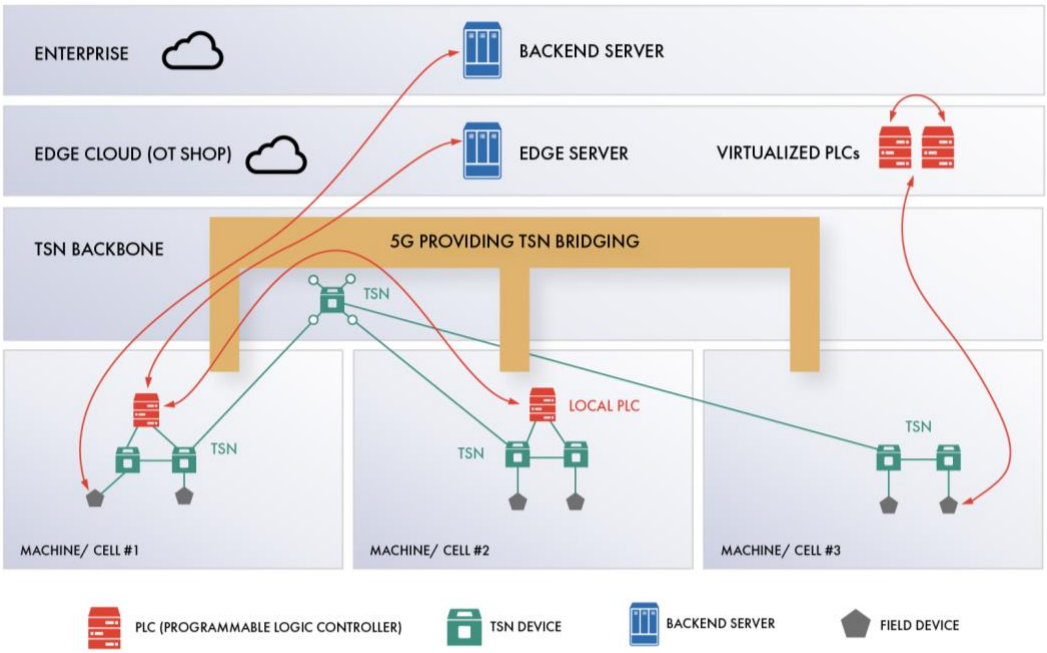

Figure 6-3: Example scenarios of TSN bridging over 5G

6.2.2 IEC Industrial Communications and Fieldbus Systems

Ethernet is a family of networking technologies commonly used today in local (LAN), metropolitan (MAN) and wide-area networks (WAN). Although the latest standards support higher bit rates and longer link distances, it cannot fulfill the deterministic and real-time connectivity requirements expected by industrial automation applications because of the carrier-sense multiple access with collision detection CSMA/CD method on Data Link Layer, which guarantees neither the arrival of an Ethernet frame nor its delivery time. The usage of full-duplex switched Ethernet can mitigate the problem but it does not solve it.

To tackle this limitation, a family of industrial network protocols used for real-time distributed control has been standardized in IEC 61158. They were designed to support the industrial computer automation system that is typically organized in a hierarchy of Programmable Logic Controllers (PLCs) being connected to sensors and actuators on the shop floor of factories and plants. Typical use case scenarios are discrete manufacturing (motion control) and process automation (chemical or pharmaceutical industry). IEC 61158 includes conventional fieldbus protocols (Profibus, Modbus-RTU, CC-Link, CANopen, DeviceNet, etc.) and evolved later to industrial Ethernet technologies, which were designed based on the standard Ethernet to meet the specific communication requirements in an industrial environment.

Figure 6-4 illustrates a few prominent industrial communication and Fieldbus protocols and their modification on stacks.

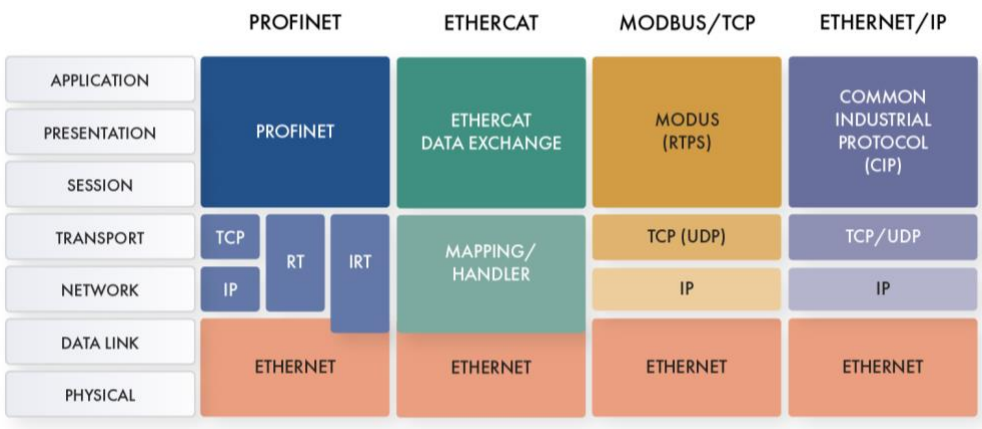

Figure 6-4: Industrial communication and Fieldbus protocols
Source: EtherCat Technology Group

EtherNet/IP is an industrial network protocol that adapts the Common Industrial Protocol (CIP) to standard Ethernet. It is one of the leading industrial protocols in the United States and is widely used in a range of industries. The EtherNet/IP and CIP technologies are managed by Open DeviceNet Vendors Association (ODVA Inc.), a global trade and standards development organization founded in 1995.

Profinet (Process Field Net) is an industry technical standard for data communication over industrial Ethernet. Profinet was invented by Siemens and is maintained and supported by Profibus & Profinet International. It supports all real-time classes including isochronous real-time (IRT), where communication takes place cyclically and is divided into several phases.

EtherCAT (Ethernet for Control Automation Technology) is based on the master-slave principle[1] and applies a procedure for the processing of cyclic data in field devices. It was invented by Beckhoff Automation and is maintained and supported by the EtherCAT Technology Group (ETG), which was established in 2003.

Modbus-TCP was developed by Schneider Electric and has been managed by the Modbus Organization since April 2004. It is designed for soft real-time applications. It is located on the application layer on top of TCP/IP and completely based on standard Ethernet components.

Other popular Industrial communication and Fieldbus systems that are not covered in this document are Powerlink, Sercos III and CC-Link IE.

[1] *https://www.ethercat.org/en/technology.html*

6.2.3 IEEE TIME-SENSITIVE NETWORKING

The Time-Sensitive Networking Task Group (TSN TG) within IEEE 802.1 Working Group deals with deterministic services through IEEE 802 networks, which aims to create a publicly available standard solution for deterministic Ethernet.

A wide range of TSN functions have been defined, among which some important functions are discussed here at a high level.

Scheduled traffic (802.1Qbv) reduces latency variation for frames with known timing. This is achieved via time-based control and programming of the bridge queues. Each queue is equipped with time-gates (time-gated queues) and the queue can be served only when the gate is open. Gate open/closed states are changed according to a periodic time schedule. This function requires time synchronization.

Asynchronous traffic shaping (P802.1Qcr) provides zero congestion loss without time synchronization. ATS is similar to per-flow IntServ shaping, except that, first, all streams from one input port to the same output port share the same queue and, second, a shaper state machine applies to a set of streams, and ensures the right shaper is used upfront of the queue. The essence of the ATS function is to smooth traffic patterns by re-shaping at every hop so that urgent traffic is prioritized over “relaxed” traffic. Strict priority queuing is used for ATS.

Frame replication and elimination for reliability (802.1CB) is targeted to avoid frame loss due to equipment failure. It is practically a per-frame 1+1 (or 1+n) redundancy function. There is no failure detection or switchover incorporated. FRER sends frames on two (or more) maximally disjoint paths, then combines the streams and deletes extra frames.

Stream reservation protocol enhancements and performance improvements (802.1Qcc): It provides Time-Sensitive Networking configuration-related attributes. Qcc describes three models for TSN user/network configuration (fully distributed, centralized network/distributed user and fully centralized model). Each model specification shows the logical flow of user/network configuration information between various entities in the network.

Table 6-2 provides a comparison between industrial Ethernet and TSN technologies, based on key characteristics and performance metrics.

	Ethernet/IP	**Profinet (IRT)**	**EtherCAT**	**Modbus-TCP**	**TSN**
Realtime Class	isochronous RT cycle time 250 µs (at 100 MB)	isochronous RT cycle time 250 µs (at 100 MB)	isochronous RT cycle time 250 µs (at 100 MB)	soft RT: scalable cycle time, approx. 100 ms	isochronous RT: scalable cycle time
Layer 2 impact	Yes	Yes	Yes	No	Yes
Min. Cycle Time	100 µs	31.25 µs	12.5 µs	15 ms	< 25 µs
Jitter	1 µs	1 µs	1 µs	1 ms	< 100 ns

Redundancy	No	Yes	Yes	No	Yes, 802.1CB
Interface Speed	10M, 100M, 1G	10M, 100M	100M, 1G, 10G	10M, 100M, 1G	10M, 100M, 1G, 2.5G, 5G, 10G
Max. # Devices	90	60	180	Unlimited	1024 per TSN domain
Openness	Open DeviceNet Vendors Association ODVA	Profibus & Profinet International	EtherCAT Technology Group ETG	Modbus Organization	IEEE 802.1, IEC/IEEE 60802

Table 6-2: Comparison of industrial Ethernet and TSN

TSN standardization is still in progress. The IEC/IEEE 60802 TSN profile for industrial automation is a joint project of IEC SC65C/MT9 and IEEE 802. This joint work will provide a dual logo standard that is both an IEC and an IEEE standard. The profiles select features, options, configurations, defaults, protocols, procedures of bridges, end stations and LANs to build industrial automation networks.

The IIC created two physical instances of a TSN testbed.[1] One is hosted in North America and the second is hosted in Germany. These testbeds are used for plugfest activities where member companies collaborate to test implementations and interoperability.

6.2.4 IEEE Short Range Wireless

Here we look at short range wireless networking namely IEEE 802.11 Wireless Local Area Network (WLAN aka Wi-Fi) and IEEE 802.15 Wireless Personal Area Networks (WPAN) that use unlicensed spectrum in the ISM-Band. In that context, short range means a few meters up to several hundred meters. The coverage area might be extended using meshed networking capabilities (Wi-SUN, Bluetooth, ZigBee). Other short-range communication protocols are not covered here (Z-Wave, RFID, NFC, Wireless M-Bus, Wireless IO-Link, DECT and IrDA).

6.2.4.1 IEEE 802.11

IEEE 802.11 Wireless Local Area Network (WLAN) is part of IEEE 802 Local Area Network protocols, and specifies a set of Physical Layers & Data Link Layers of Wireless Local Area Networks in different unlicensed frequency bands, mainly in 2.4 and 5GHz frequency range. Developed and established since 1997, it is the world's most widely adopted wireless networking standard, used in most home, office, hotspot and campus networks to allow devices to connect to local networks and to access the Internet.

The IEEE 802.11 family of standards, as shown in Figure 6-5, consist of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The 802.11 protocol family

[1] *https://www.iiconsortium.org/time-sensitive-networks.htm*

employ carrier-sense multiple access with collision avoidance whereby equipment listens to a channel for other users before transmitting data (listen before talk). The Wi-Fi standard is managed by the Wi-Fi Alliance.

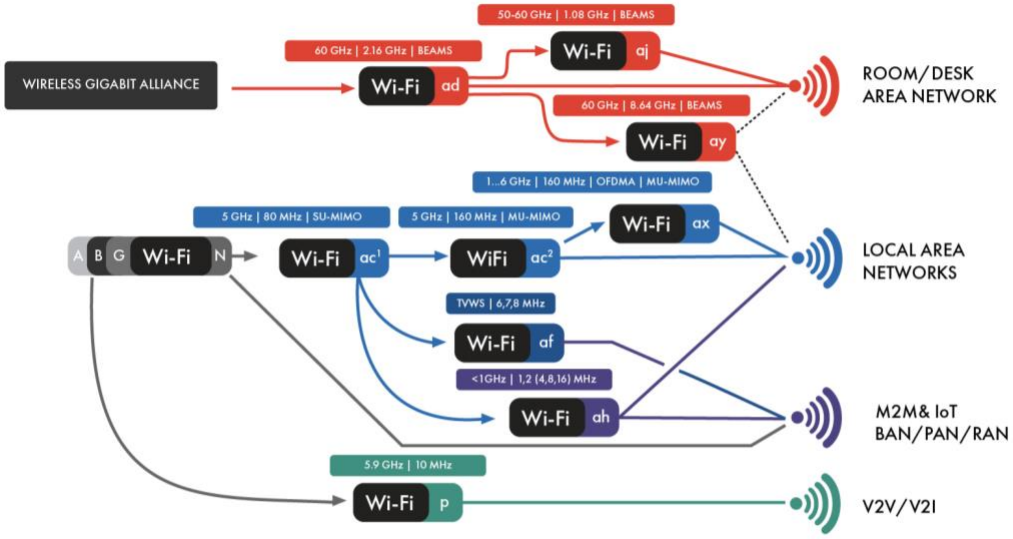

Figure 6-5: IEEE 802.11 Wireless Local Area Network/Wi-Fi family
Adapted from Rhode & Schwarz

The main versions are IEEE 802.11a/b/g/n and ac (renamed to Wi-Fi 1, 2, 3, 4 and 5). The most recent family member is IEEE 802.11ax (renamed to Wi-Fi 6), which provides the following enhancements compared to previous Wi-Fi versions:

OFDMA DL/UL with lower latency; more supported devices per access point; more capacity and more efficient use of spectrum and network resources in dense environments.

Long OFDM symbol with higher efficiency and capacity, and improved outdoor performance (4x increase in data speed at the cell boundaries).

8x8 MU-MIMO DL/UL serves up to 8 simultaneous users, doubling capacity over 4x4 MIMO, in both directions.

1024 QAM with higher per-device peak speed, higher capacity (+25% vs 256 QAM) and more efficient use of network resources.

Uplink resource scheduling provides better management of network resources, lower latency, better support and performance in dense environments and an increased battery life.

BSS color provides better spatial frequency reuse by coordination among neighboring access points and increased capacity in dense and high-traffic environments.

Target wake time allows for device-specific, more flexible management of wake/sleep cycles and a longer battery life for IoT applications.

6 GHz band support provides more spectrum available to Wi-Fi (also refer to Wi-Fi 6e) and more capacity and ability to serve more diverse use cases.

Wi-Fi Protected Access WPA3 provides increased security by longer encryption keys (128 or 192-bit) and forward secrecy. It also replaces Pre-Shared Key exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016.

6.2.4.2 IEEE BLUETOOTH

Bluetooth defines the physical and the data link layers for wireless connectivity with devices within or entering personal operating space (PAN–Personal Area Network). Bluetooth was originally invented by Ericsson. The Bluetooth standards originate from IEEE 802.15 but are now managed by the Bluetooth Special Interest Group (SIG). To market Bluetooth-enabled devices a manufacturer must license and comply to the Bluetooth SIG standards. Bluetooth typically operates in the unlicensed band at 2.4 GHz, which is crowded today and prone to interference from other devices.

Bluetooth uses a radio technology called frequency-hopping spread spectrum. Range is power-class-dependent, but ranges vary in practice from 1 to 100m. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth 1 MHz channels (or 40 2 MHz channels for Bluetooth Low Energy). It usually performs 1600 hops per second, with adaptive frequency-hopping (AFH) enabled. Bluetooth Basic Rate (BR) and Enhanced Data Rate (EDR) use different modulation schemes (GFSK and DPSK) and achieve transmission rates of 1~ 3 Mbps. In theory, newer versions of Bluetooth can achieve data transfer speeds of up to 24 Mbps.

To use Bluetooth wireless technology, a device must be able to interpret certain Bluetooth profiles, which are definitions of possible applications and specify general behaviors that Bluetooth-enabled devices use to communicate with other Bluetooth devices. These profiles include settings to parameterize and control the communication from the start. Adherence to profiles saves time transmitting the parameters anew before the bi-directional link becomes effective.

There are a wide range of Bluetooth profiles that describe many different types of applications or use cases for devices. The latest version of Bluetooth standard is 5.2, which was released in November 2019. Today, Bluetooth is supported by a wide range of consumer and industrial devices.

6.2.4.3 IEEE 802.15.4

IEEE 802.15.4 Low Rate WPAN is designed for low-cost and low-speed ubiquitous communication between devices and is maintained by the IEEE 802.15 working group, which defined the standard in 2003. It describes the physical and the data link layers for wireless protocols like Zigbee, ISA100.11a, WirelessHART, MiWi, Thread and SNAP, which specify the upper layers of the related protocol stack. In particular, 6LoWPAN defines a binding for the IPv6 version of the IP

over WPANs and is itself used by upper layers like Thread. The basic framework conceives a 10m communications range with a transfer rate of 250 kbps. There are variations of the physical layer with even lower power requirements with transfer rates of 20, 40 and 100 kbps. Important features include real-time suitability by reservation of guaranteed time slots, collision avoidance through carrier-sense multiple access with collision avoidance CSMA/CA and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection. The standard does have provisions for supporting time and rate sensitive applications because of its ability to operate in pure CSMA/CA or time division multiple access TDMA modes. IEEE 802.15.4 conformant devices may use one of three possible frequency bands for operation (868/915/2450 MHz).

Later amendments to 802.15.4 include updates for Field Area networking. These amendments include 802.15.4g, 802.15.4v, 802.15.4x and 802.15.4e. 802.15.4g added PHY's including SUN-OQPSK, SUN-FSK and SUN-OFDM with data rates from 10kbps to 800kbps. 802.15.4x further defined additional capabilities to 2.4 Mbps.

6.2.5 LONG RANGE WIRELESS

Some non-critical IoT applications with relaxed telemetry-type requirements can use Low Power Wide Area Networks (LPWAN), which describe terrestrial wireless networks for long-range communication and data transmission at ultra-low bit rates. It fills a low-end gap in the existing technologies and targets low-cost deployment of IoT for niche applications such as tracking and metering. LPWAN devices use low complexity and low-cost hardware, often powered by batteries and can therefore operate in the field up to years. Requirements and applications of LPWAN are similar to NB-IoT and CAT-M1 of 3GPP.

LPWAN technologies are primarily operating in unlicensed spectrum and typically in sub-GHz ISM-Bands where signal propagation is beneficial to achieve longer range while still using relatively little power. Available bands vary across countries and regions. Using unlicensed spectrum is more prone to interference compared to technologies working in licensed spectrum bands. LPWAN providers either provide network services where the leading example is Sigfox,[1] or technology such as chipsets and designs, with LoRA[2] being the prime example based on Semtech's closed technology. LPWAN is based on a single-provider solution with ecosystems of partners based on proprietary technology that is neither openly standardized nor interoperable. The coverage and service availability of LPWAN needs to be investigated and verified on a market-by-market (e.g. countries, regions) basis, or by specific geographical locations.

The technical characteristics of LoRa include data rates of 0.3 kbps ~ 50 kbps, a range of 3 ~ 5 km in dense urban areas and up to 30 km in rural areas. Sigfox is an ultra-narrowband service designed for very low throughput and small packets of up to 12 bytes uplink and 8 bytes

[1] *https://www.sigfox.com/en*
[2] *https://lora-alliance.org/*

downlink, and with the number of packets per device limited to 14 packets per day. The range is up to 40 km in open field.

6.2.6 SATELLITE

Satellite communication technology has two main use cases. In the first, IIoT devices are spread over very large areas, creating a network with very low node density. To connect them with terrestrial wired or wireless technologies would be challenging, both from a technical and economic perspective. In the second, deployment of terrestrial systems is technically or economically unfeasible. This is the case for remote, unpopulated areas of the land, the majority of seas, and all oceans. Together, these areas constitute more than 80% of Earth's surface. Hence, connecting aircrafts and ships can be achieved only with satellites.

The main advantage of satellites over terrestrial networks is their wide coverage, on a regional and continental scale. GEO (geostationary earth orbit) and equatorial medium earth orbit (MEO) constellations can provide a continuous coverage belt around the world, from the equator to mid-latitudes, leaving only the polar regions unconnected. These gaps can be filled with near-polar low earth orbit (LEO) constellations or dedicated Molniya orbit satellite systems[1]. LEO constellations can also provide fully global coverage on their own.

The main challenge in connecting IIoT devices via the satellites is closing the link budget over large distance. The lowest LEO satellites operate at the altitude of around 300 km. MEO satellites orbit at around 8,000 km and GEO satellites at 35,000 km. IIoT devices are small and often battery powered, so they usually don't have high-gain antennas, nor sufficient RF power to reach high altitudes. Consequently, satellite technology can support IIoT in two modes: as a direct radio access network with LEO satellites (up to 700 km) and as a backhaul technology for other wireless or wired networks (any altitude).

Direct radio access: Satellites using these technologies usually fly not higher than 600 km and use L-band or S-band. Higher frequencies than S-band are rarely used for direct access IIoT due to the high signal loss.

For direct radio access via satellite, coverage is not the most appropriate metric for assessing implementations. Provision of truly global continuous coverage from LEO requires hundreds of satellites and would rarely close the business case. However, in case of IIoT devices not requiring real-time connectivity, 12-hour revisit time can be provided with a single LEO satellite in a near-polar orbit. This interval can be brought down to minutes with an increasing number of satellites. During contact, the satellite receives a data burst from the device and stores it onboard. At the next contact with a ground station (usually less than 90 minutes later), it downlinks the data it collected during the previous orbit. This mode is also called store & forward.

[1] *https://en.wikipedia.org/wiki/Molniya_orbit*

Direct Radio Access LEO satellites either use established LPWA technology like Eutelsat ELO (Sigfox), Lacuna Space (LoRaWAN) and OQ Technology (NB-IoT) or proprietary and undisclosed technologies (Echostar Heilos Wire, Iridium, Kepler, Xingyun).

Satellite backhaul: Satellites can be used to backhaul the signals from isolated IIoT networks, connecting them with parent corporate networks or the internet. Usage scenarios may include stationary IIoT terrestrial networks at industrial sites, remote mines or offshore oil rigs. They may also include on-board IIoT networks on aircraft, ships and land vehicles. For small traffic, the backhaul may go through narrowband satellite systems like Iridium, Globalstar or Orbcomm. For higher traffic, broadband LEO satellite systems can be used, like GEO HTS (Inmarsat, SES, Eutelsat, Thuraya, etc.), MEO (O3b) and LEO (KLEO Connect, OneWeb, Starlink, Telesat LEO, Kuiper). Finally, dedicated IoT backhaul solutions are being developed (Kepler).

The satellite terminals are placed on the ground, on buildings, masts or vehicles. The terminals then use any terrestrial IIoT access technology to aggregate IIoT traffic. Another option is to place the terminal on a High-Altitude Platform Station (HAPS), providing a LPWA Radio Access to the IIoT devices in a large area below it.

LEO Satellite backhaul allows true real-time connectivity between IIoT devices, the cloud and the applications using them.

6.3 INTERNETWORKING STANDARDS AND TECHNOLOGIES

6.3.1 DETERMINISTIC NETWORKING (DETNET)

The IETF Deterministic Networking (DetNet) Working Group[1] focuses on deterministic unicast or multicast data flows that operate over Layer 2 bridged and Layer 3 routed segments, where such flows can provide bounds on latency, loss, packet delay variation (jitter), and high reliability.

DetNet operates at the IP/MPLS layer and it is for networks that are under a single administrative control or within a closed group of administrative control. Nevertheless, DetNet is not intended for large groups of domains such as the internet.

DetNet functionality is implemented in two adjacent sub-layers in the protocol stack:

DetNet service sub-layer: This provides DetNet service to higher layers in the protocol stack and applications including service protection, packet sequencing, duplicate elimination, flow replication/merging and packet encoding/decoding.

DetNet forwarding layer: This supports DetNet service in the underlying network to DetNet flows including resource allocation, explicit routes and congestion protection.

As shown in Figure 6-6, a deterministic network defined in DetNet comprises:

[1] *https://datatracker.ietf.org/wg/detnet/about/*

- DetNet (enabled) end systems: aka “host” (IETF), and an “end station” (IEEE 802),
- DetNet relay nodes including a DetNet service sub-layer function and a DetNet forwarding sub-layer functions,
- DetNet edge nodes, a DetNet relay node that acts as a source or destination at the DetNet service sub-layer and
- DetNet transit nodes operating at the DetNet forwarding sub-layer and providing congestion protection over those paths.

All DetNet nodes are connected to sub-networks. A point-to-point link is treated also as a simple sub-network. Sub-networks provide DetNet compatible service for support of DetNet traffic. Multi-layer DetNet systems may also be possible, where one DetNet network appears as a sub-network, and provides service to a higher layer DetNet system.

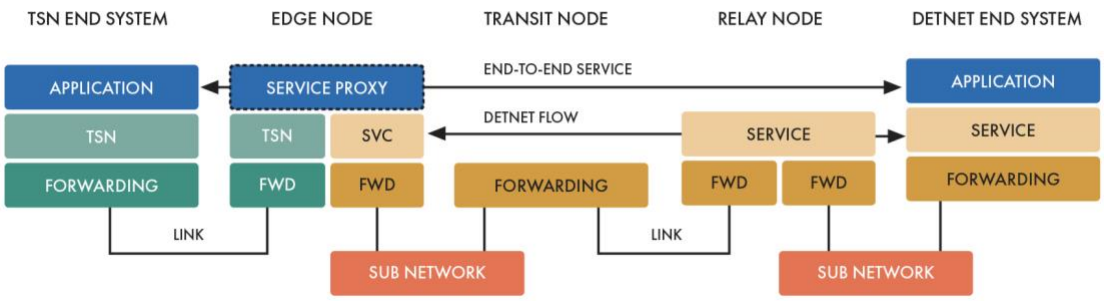

Figure 6-6: A simple DetNet enabled network

DetNet standardization is still in progress. There are also some challenges and requirements of DetNet that need to be addressed by future work, such as tolerance of time deviation, long-link propagation delay and massive dynamic flows. There is close cooperation between IETF DetNet WG and IEEE802.1 TSN to ensure interoperability and to simplify implementation of deterministic functions working for both Layer 2 and Layer 3 and to complement each other if necessary.

6.3.2 IP Transport over Low Power Wireless Networks

IP for smart objects seeks to extend IP networking into resource-constrained devices over a wide range of low-power link technologies. IEEE 802.15.4 represents one such link. Extending IP to low-power, wireless personal area networks (LoWPANs) were once considered impractical because these networks are highly constrained and must operate unattended for multiyear lifetimes on modest batteries. Many vendors embraced proprietary protocols, assuming that IP was too resource-intensive to be scaled down to operate on the microcontrollers and low-power wireless links used in LoWPAN settings.

6LoWPAN introduces an adaptation layer between the IP stacks link and network layers to enable efficient transmission of IPv6 datagrams over 802.15.4 links, thus dramatically reducing the IP overhead. The adaptation layer is an IETF proposed standard and provides header compression

to reduce transmission overhead, fragmentation to support the IPv6 minimum MTU requirement and support for layer-two forwarding to deliver and IPv6 datagram over multiple radio hops. 6LoWPAN achieves low overhead by applying cross-layer optimizations; it uses information in the link and adaptation layers to compress network- and transport-layer headers. Drawing on IPv6 extension headers, it employs the header stacking principle to separate the orthogonal concepts and keep the header small and easy to parse.

6LoWPAN network architecture: By communicating natively with IP, 6LoWPAN networks are connected to other IP networks simply by using IP routers. 6LoWPANs will typically operate on the edge, acting as stub networks. The 6LoWPAN may be connected to other IP networks through one or more border routers that forward IP datagrams between different media. Connectivity to other IP networks may be provided through any arbitrary link, including Ethernet, Wi-Fi, GPRS or satellite. Because 6LoWPAN only specifies operation of IPv6 over IEEE 802.15.4, border routers may also implement Stateless IP/ICMP Translation or other IPv6 transition mechanisms to connect 6LoWPAN networks to IPv4 networks. These IPv6 transition mechanisms do not require 6LoWPAN nodes to implement IPv4 in whole or in part.

6lo (IPv6 over networks of resource-constrained nodes): As IoT services become more popular, the IETF established the 6lo working group to study IPv6 over various link layer technologies such as Bluetooth Low Energy (Bluetooth LE), ITU-T G.9959 (Z-Wave), Digital Enhanced Cordless Telecommunications - Ultra Low Energy (DECT-ULE), Master-Slave/Token Passing (MS/TP), Near Field Communication (NFC), Power Line Communication (PLC) and IEEE 802.15.4e (TSCH). IPv6 stacks for constrained node networks use a variation of the 6LoWPAN stack applied to each particular link layer technology.

The IETF 6lo Working Group works on:

- IPv6-over-foo adaptation layer specifications using 6LoWPAN technologies (RFC 4944, RFC 6282, RFC 6775) for link layer technologies of interest in constrained node networks,
- information and data models (MIB modules, etc.) for these adaptation layers for basic monitoring and troubleshooting,
- specifications, such as low-complexity header compression, that are applicable to more than one adaptation layer specification and
- maintenance and informational documents required for the existing IETF specifications in this space.

6.3.3 SD-WAN

Software-defined WAN (SD-WAN) network is a new WAN network that can achieve its purpose by virtualization technology, application-level strategy and overlay network, on-site customer-premises equipment. The ultimate goal of SD-WAN is to replace expensive private lines with cheap links, such as MPLS.

SD-WAN is an important emerging network market, which virtualizes enterprise network services, delivers them on industry standard hardware (also known as commercial off-the-shelf hardware) and configures and delivers them from the cloud. At present, SD-WAN technology is being standardized in MEF. MEF is working to standardize SD-WAN terminology, service components, reference architectures, lifecycle service orchestration API's and SD-WAN service definition.

MEF 3.0 specification defines the overall architecture of SD-WAN (Figure 6-7) and the functional definitions and interfaces of each component.

- SD-WAN Edge: Physical or virtual
- SD-WAN Gateway: Between SD-WAN and external connectivity services
- SD-WAN Controller: Centralized management of SD-WAN edges & gateways
- Service Orchestrator: Lifecycle Service Orchestration of SD-WAN and other services
- Subscriber Web Portal: Subscriber service ordering and modification

The fundamental characteristics defined in the MEF 3.0 specification include but are not limited to the following items:

Secure, IP-based virtual overlay network: To ensure security, in addition to providing IPSec tunnels, firewalls and NAT capabilities are also required.

Transport-independence of underlay network: SD-WAN is independent of basic transport network technology and operates over any type of wireline or wireless access networks.

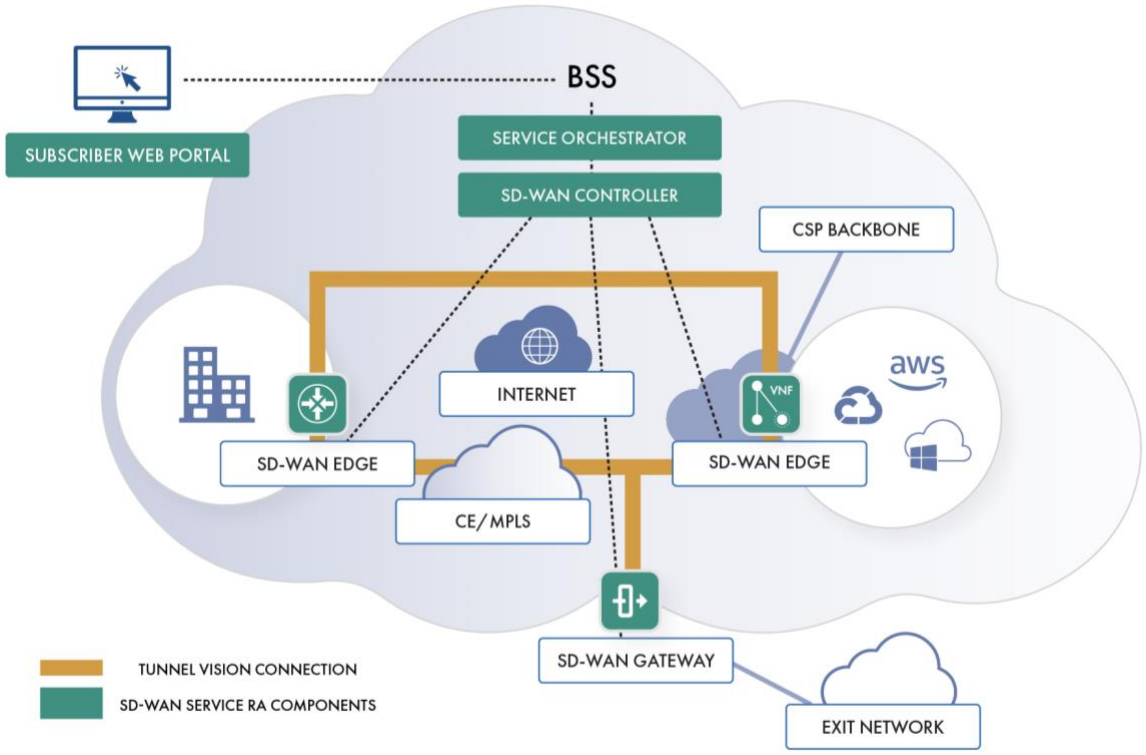

Figure 6-7: SD-WAN architecture

Service assurance of each SD-WAN tunnel: QoS performance, such as packet loss and packet latency, is measured over each SD-WAN tunnel in real-time. These measurements determine whether a particular WAN meets the performance requirements of an application resulting in application-based performance assurance.

Application-driven packet forwarding: The WAN tunnel selection is determined by an application's QoS, security or business policy requirements.

High availability through multiple WANs: SD-WANs support packet forwarding over one or more WANs at each site.

With the development of the business of industrial manufacturing enterprises, there may be new business requirements for SD-WAN. SD-WAN may also provide more technical possibilities for the development of information technology in industrial manufacturing enterprises.

7 Case Solution Examples

7.1 Case Solution Examples #1: Smart Factory Network

7.1.1 General Description

The smart factory network case solution example is part of the IIC Manufacturing Domain. New technologies like industrial IoT, virtualization, cloud and edge computing, cyber-physical systems,

digital twins, big data analytics and artificial intelligence together with new networking technologies are applied to build modern, flexible and highly automated smart factory, often referred to as Industry4.0. In this concept, machines and production assets are augmented with ubiquitous connectivity, sensors and compute capabilities, connected to a system that can monitor, visualize and manage the entire production line and make autonomous decisions. It can be understood as the digital transformation in manufacturing industry, specifically for product and service offerings and to establish new platform driven business models.

The highly specific field bus technologies that have been used in the past decades are expected to migrate to standardized network technologies like Ethernet/TSN and 5G, which are considered key network technologies to enable Industry4.0. The network key-characteristics for that view are highly reliable and deterministic communication service, high data rates, seamless mobility support, private networks support and global availability. In this example, we follow the methodology defined in the IINF to narrow down the considered network technology choices.

7.1.2 Business Concerns and Requirements

Total cost of ownership: There are a variety of choices on how to finance and operate the network. From complete do-it-yourself with rent or buy, to partially outsourcing up to completely consume “as-a-service”, all options are feasible. When using licensed spectrum, the related license fees need to be considered as well. The costs for the license fees depend typically on the size of the area that needs to be covered, the timeframe and the amount of spectrum used.

Operational model: In the past it was only possible to build up a private cellular campus network using either unlicensed spectrum (LTE-U/Multefire) or licensed spectrum from a national wireless network provider. Each came with its own challenges and drawbacks, which resulted in very limited adoption among global factory networks. With the availability of licensed spectrum for local use this is expected to change with the introduction of 5G. 5G-ACIA defined several deployment options that result in different business models. Either the Non-Public Network (NPN) [5G-ACIA] is deployed as an isolated private campus network or as Public Network Integrated NPN (PNI-NPN). The integration options are Sharing RAN, Sharing RAN & Control or NPN within Public Network. In the case of Public Network Integration, network security, service-level agreement and liability need to be clarified with the public network operator. Another consideration is whether the factory data can leave the private campus network or not.

Regulatory aspects: For wireless technologies, either unlicensed frequency spectrum (e.g. WiFi) or licensed frequency spectrum (cellular network) are used, which are subject to national, regional or global regulations. This is why WiFi technology works everywhere in the world, but it also means that it can be used by everyone, which could lead to network interference resulting in poor network performance. 5G networks rely on licensed spectrum which eliminates the interference challenges seen in unlicensed. Mobile networks operators are in a prime position to partner with industries to provide 5G cellular wireless private campus/factory networks. In some countries, a further alternative can be local licenses for industries, and for this purpose, mid-band

(2575 ~ 3800 MHz) or high-band frequencies (mmWave 24.25 ~ 29.1 GHz). Spectrum licenses for local use are available in France, Germany, Japan, Hong Kong, UK and US (Citizens Broadband Radio Service - CBRS). As of January 2021, other countries considering to follow this approach are Australia, Brazil, Chile, China, Croatia, Finland, Luxembourg, Malaysia, Netherlands, Norway, Poland, Slovenia and Sweden. The Global Mobile Suppliers Association[1] is tracking the progress on private spectrum assignment.

Technology governance: To avoid vendor lock-in, single-sourcing and limited availability in certain regions global open standards are imperative. Factory owners operate in different countries and regions, and therefore need a network solution that can be used globally without restrictions. Proprietary technologies limit the choices and cannot guarantee a robust supply chain. Further, they restrict the creation of a prospering and healthy ecosystem.

Licensed spectrum for private mobile campus networks is a new opportunity for manufacturing. It is expected that mobile networking technologies will play a more important role in smart factory networks. Specifically, for 5G it is predicted that the market in manufacturing will reach $10.8bn by 2030 (ABI Research, 2020). Details are subject to national regulation and must be considered individually.

7.1.3 Usage Concerns and Requirements

Deployment context: First, we must define whether the new network technologies should be implemented in an existing factory with integration of new and legacy production assets (brownfield) or in a new factory (greenfield). The brownfield approach is more complex as migration aspects of production assets and processes need to be considered, which may lead to a phased approach. Further, it needs to be defined in which areas of the factory the new network technology should be deployed. Outdoor areas, office areas, shop floor and warehouse have all different environmental conditions (temperature, fire, explosion, humidity, water, particles, chemicals, mechanical stress, electromechanical interference) that require different safety, protection and certification measures and might affect network planning and deployment. For example, International Protection class IP20 might be fine for the office areas and the warehouse but is not sufficient for outdoor areas and shop floor where ruggedized equipment with International Protection class IP67 might be required. Different networking technologies may be implemented in different areas of the factory. For example, 5G is needed in the production hall and warehouse, whereas WiFi-6 is sufficient for the office areas. 5G also supports positioning and tracking with sub-meter accuracy so dedicated beacon infrastructure for Bluetooth or UWB might not be necessary.

Lifecycle perspective: Lifetime of OT and mechanical systems are typically much longer (>>10 years) than the lifetime of CT (5 ~ 10 years) and IT (3 ~ 5 years) systems. This implies that OT

[1] *https://gsacom.com/*

systems need to provide the flexibility to upgrade their communication and computing capabilities to “retro-fit” to new use cases, scenarios and technologies. The advent of cyber-physical systems, will likely shorten the lifecycle in the OT domain significantly.

Operation & management: Important O&M questions need to be addressed to ensure that the network can be operated and maintained in an efficient way, for instance, how to provision new devices? How to monitor network faults, performance and efficiency? How to maintain the system and install new software/firmware? How to gather operational data? How to do network asset and lifecycle management?

Security: The smart factory owner must ensure a secure operation. Examples for operational technology security features are physically isolated networks, users/equipment/processes forming a single trust domain within perimeter, non-authenticated mechanisms/secure hardware for subscriber and regulatory compliance (IEC 62443). Examples for 5G security features are authentication methods (5G-AKA and others), network slicing (for separation and segregation), secure storage of credentials (USIM), protection against jamming and interception.

Conclusions from the usage viewpoint insights are that the networking technologies are easy to deploy and can be operated and maintained with reasonable efforts. The increase of the level of production flexibility and autonomy also needs to be reflected by the underlying smart factory network as it is a technology enabler and the foundation for Industry4.0. The network technologies need to be flexibly deployed in challenging indoor and outdoor environments and security or safety threats need to be prevented as much as possible.

7.1.4 USE CASES AND TECHNOLOGY CONSIDERATIONS

New technologies are introduced like mobile devices, data platforms and edge/cloud computing to realize the vision of a smart factory. The challenges of Industry4.0 include economic, social, political and organizational factors. To support the industrial internet, we must transform heterogeneous and proprietary technologies to open global standards to support IT/OT convergence. Even today, wireline networking technologies dominate in the manufacturing industries, but as factories get away from conveyer belts towards more flexible production methods, more mobile production assets are introduced (mobile robots/cobots and automated guided vehicles). Wireless technologies like Wi-Fi, Bluetooth, LTE and MulteFire have been introduced with mixed success due to their limited capability to serve demanding use cases in terms of mobility, latency, jitter and reliability.

Table 7-1 shows a selection of typical use cases and their related networking requirements, which were listed in section 4.2 on Requirements. Network coverage is not considered in the table as it is assumed that a proper network planning is done for the small cells/access point to provide good local coverage where needed. A similar table can be found on page 10 of the 5G-ACIA whitepaper on 5G for Connected Industries and Automation [5G-CON].

	Condition Monitoring	Motion Control	Automated Guided Vehicles	Process Automation	Augmented Reality	Functional Safety
Latency	20-100ms	0,1-1ms	10-20ms	50ms	10ms	10ms
Determinism	No	Yes	Yes	Yes	Yes	Yes
Time Synchronization	No	Yes	Yes	No	Yes	No
Availability	99.99%	99.9999%	99.9999%	99.99%	99.99%	99.9999%
Redundancy	No	Yes	Yes	Yes	No	Yes
Mobility	Yes	No	Yes	Yes	Yes	Yes
Peak Data Rates	< 1 Mbps	100 Mbps	100 Mbps	10 Mbps	1 Gbps	< 1 Mbps
Battery Power	Up to 10 years	Mains powered	Up to 8h	Up to 10 years	2 – 3h	Up to 10 years
Connection Density (per 1000 m^2)	1000	100	200	1000	50	100

Table 7-1: Selected industrial applications in manufacturing and their networking requirements.

Most of these use cases can be covered by wireless technology. However, some very demanding use cases like motion control, with cycle times of 250µs, and the realization of functional safety is not yet supported. To cover those use cases, wireline connectivity to manufacturing assets is still needed in modern smart factories. Ethernet/TSN is a powerful networking technology to realize these kinds of use cases and to substitute legacy fieldbus systems where possible.

7.1.5 Architecture and Design Considerations

In the past decades, the Purdue Enterprise Reference Architecture (PERA) model, also referred to as “automation pyramid”, has been widely adopted in the manufacturing and process industry. It structures the different functions in a factory into different layers of a hierarchical model. The different layers are isolated and protected to ensure security requirements. The factory shop floor and the factory office network are strictly separated by a de-militarized zone. Sensitive information and data need to be protected and should stay on-site to increase security.

We assume that the five hierarchal layers of the conventional automation pyramid are flattened due to IT/OT convergence. Virtualized network functions, programmable logic controllers and data collection, aggregation and analytic functions can be flexibly orchestrated on demand to different network layers by means of distributed computing in the edge. Systems like Enterprise Resource Planning (ERP), Supply Chain Management (SCM) and Product Lifecycle Management (PLM) are deployed in the IT domain (Level 4&5), whereas Manufacturing Execution System (MES), Supervisory Control and Data Acquisition (SCADA), HMI, production domain and cell

controllers can be located in the underlying OT layer (Level 0 ~ 3). The next stage of development is to virtualize those OT functions and to orchestrate them flexibly on the edge node where needed. An example of the potential target architecture is shown in Figure 7-1. Here, in each cell/area/zone WiFi-6, 5G and Ethernet/TSN are assumed depending on the use cases requirements (as outlined in section 7.1.3 on Deployment Context).

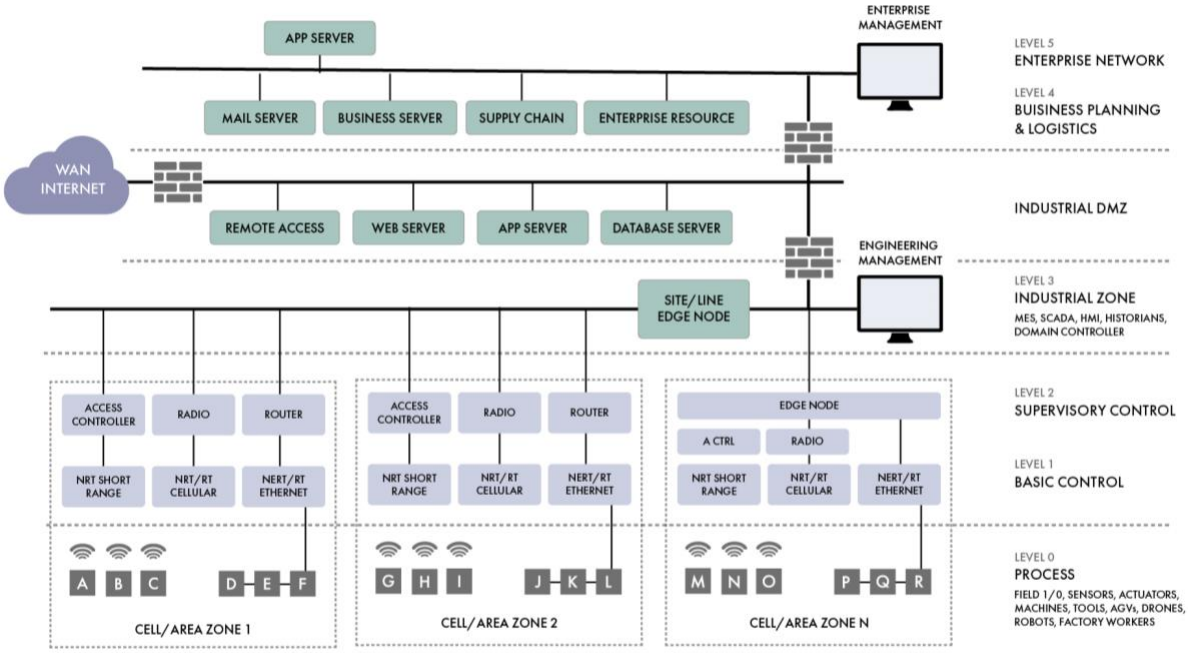

Figure 7-1: Example of target network architecture for smart factory

7.1.6 Network Technology Recommendations and Conclusion

With this example we applied the methodology described in chapter 2 and 3 of the IINF to make our conclusions and network technology recommendations.

To increase flexibility and reduce overall complexity, established heterogeneous network technologies need to converge to unified, modern and open network infrastructures. In the mid-to-long term perspective, it is assumed that the established fieldbus systems will be substituted by new wireline and wireless networking technologies. OPC Unified Architecture is relevant for the manufacturing industry in the upper layer, for example, when connecting controllers to each other or to the cloud, and different communication models are supported like client/server or publish/subscribe. There are industry efforts to make it real-time capable and to bring it to the field layer, which is handled in the recently established Field Layer Communication group of OPC Foundation. Further OPC UA also connects to different cloud domains of different parties (other service providers, partners, users and suppliers), which is referred to as cloud-to-cloud or federated cloud connectivity.

Conclusion for wireless network technologies in smart factory networks: 5G is a promising candidate to fulfill most requirements of the scenarios listed in Figure 7-1 above. In contrast to previous cellular systems like UMTS and LTE, it is more powerful and designed specifically for industrial use and in difficult environment and critical infrastructure. This is due to its capabilities introduced with 3GPP Release 16 like massive and critical Machine-Type-Communication (mMTC and cMTC/URLLC), positioning and Non-Public Network support.

Wireless short-range and long-range communication may be important too for non-deterministic communication, using a wide range of unlicensed spectrum. This would complement the 5G network infrastructure and stepwise migrate to a unified and commoditized wireless network with decreasing costs and increasing technology adoption.

Conclusion for wireline network technologies in smart factory networks: Wireless networking technologies may make limited sense with big or static production assets that do not need to move in the environment, or that need to be connected to mains power due to its energy demand. Examples are metal sheet presses, CNC machines, 3D printers (additive manufacturing) and packaging machines. The motion-control use cases fit well to the requirements for packaging lines from the Manufacturing of Consumer-Packaged Goods (CPG) scenario from section 3.1.

For wireline communication, we can assume that it stays important as some networking requirements can't be fulfilled by wireless technologies (motion control with latency << 1ms) and some scenarios don't need mobility at all. It is assumed that today's field bus systems are migrating towards Ethernet based technologies like TSN and Deterministic IP Networking. This could also be a step-by-step approach by transparently tunneling between legacy parts of the network to enable brownfield innovation scenarios. A promising development for the wireline physical layer is Single Pair Ethernet IEEE 802.3cg, which reduces complexity and cost. Depending on the length of the cable, it can achieve data rates of up to 1 Gbps.

For the smart factory backbone, a fiber optical network is likely the best suggestion. Wireless access points need to be connected with several Gbps and for the aggregation and core network interfaces toward the on-premises data center up to 100 Gbps are used.

7.2 Case Solution Examples #2: Smart Grid

7.2.1 General Description

In Smart Grid, metrology and various grid-connected assets are augmented with ubiquitous connectivity while connected to a system that can monitor, visualize and manage the grid and make autonomous decisions. This technology allows for automated meter reading, electric distribution system automation, electric system outage detection and other use cases including: remote power disconnect, theft detection, net metering and pre-pay electricity services.

For a more thorough explanation of Smart Grid use cases, see the work from the Utilities Communications Association international *users' group* on network system requirements

specification [UCA-NET], latency and security requirements [UCA-SEC] and diagrams illustrating all possible paths for network communications in the smart grid [UCA-PATH].

7.2.2 BUSINESS CONCERNS AND REQUIREMENTS

Total cost of ownership: Based on the networking options available, CAPEX-related costs mainly involve equipment purchases and technology licenses. As in other domains, trade-offs exist between cost and metrics like reliability and coverage. For example, while unlicensed microwave spectrum incurs a lower cost, it risks possible interference with other technologies, e.g. 2.4 GHz is also used by Wi-Fi and ZigBee. Higher frequencies tend to have less potential interference, but also a significantly reduced range. Licensed microwave links on the other hand require a license (e.g. FCC in the USA), they use better (and more expensive) antennas to focus transmissions more effectively, and incur higher installation costs. But they offer greater reliability due to a guarantee of no interference, and depending on the equipment, they can offer higher data rates. From an OPEX point of view, costs vary depending on whether the smart grid providers can operate their own installations (e.g. using PLC) or resort to paying for third party network services. Obviously, with automated meter reading, labor costs are reduced by the elimination of manual meter reading. There are a number of intangible benefits from Smart Grid applications that allow for better recognition of electric system outages, faster electric system outage restorations, energy theft detection and pre-pay services. There are a number of future use cases that could allow for microgrids, smart cities along with a canopy network that could include gas and water meters.

Operational model: The model for how most utilities operate is a regulated monopoly. As a regulated entity, utilities usually get return on their investments from investments made into maintaining, updating and improving their electric, water or gas infrastructure. Smart Grid use cases optimize operational efficiencies, contribute to higher grid reliability and can reduce carbon footprints with distributed energy resources. The deployment choice will result in different business models depending on total cost of ownership above. The decision on which solution to adopt (own installation or outsourced) would largely depend on the part of the infrastructure and the smart grid application under consideration. For example, third party networking services, such as cellular communication, can be better suited for advanced metering and satellite communication for remote locations, as opposed to investing to own infrastructure. Given the variety of smart grid applications and their requirements and the large geographic span of energy infrastructure, networking will likely be a combination of privately owned and outsourced solutions that balance the cost with requirements such as reliability, performance and security.

Regulatory aspects: For wireless technologies either unlicensed frequency spectrum (e.g. WiFi, Wi-SUN) or licensed frequency spectrum (e.g. cellular network) are used. Utilities have access to dedicated licensed wireless bands in certain regions in the world. To date, most smart grid solutions have been deployed in the North America in the 900 MHz unlicensed bands with link speeds ranging from 19.2 Kbps to 250 Kbps. Internationally (especially Europe) 800 MHz unlicensed bands are used if 900 MHz is not available. There are few examples of licensed

spectrum usage that have been directed toward automatic meter reading and control. These involve the use of WiMAX at 930 MHz, with high data speeds (up to 75 Mbps), and include SP AusNet an Australian energy delivery company and the world's largest WiMAX vendor Alvarion (in partnership with US utility company National Grid).

Technology governance: To avoid vendor lock-in, single-sourcing and restricted availability in certain regions global open standards are imperative. Utilities have regulatory requirements that depend their regulators. Requirements on security, data privacy and ownership of said data vary. Utilities usually do not have requirements for operation on licensed and unlicensed spectrum. The most prevalent communication technologies used in the smart grid have been developed by standards development organizations, e.g. IEEE, NIST, ANSI, IEC and ITU. In addition, there are a number of alliances that recognize the value of a particular technology and attempt to promote specifications as standards for that technology. Some well-known alliances related to the utility industry include ZigBee, WiFi and HomePlug Powerline.

7.2.3 USAGE CONCERNS AND REQUIREMENTS

Deployment context: Due to the large geographic span of the smart grid infrastructure and that most of it is outdoors, environmental conditions need to be considered, such as temperature, humidity, and sources of interference. Terrain, landscape and vegetation also affect the decision. This also depends on the infrastructure and the application. For example, extensive coverage of satellite communication suits keeping track of electric-vehicle-related information.

Lifecycle perspective: The lifetime of utility deployed assets is typically 15 ~ 20 years.

Operation & management: While offline resource provisioning is important to meet expected performance requirements, real-time operations are key in enabling dynamic scenarios in distributed settings, such as electric vehicle charging. Equally important are efficient monitoring solutions that can detect faults, e.g. as a result of natural disasters (with subsequent triggering of resource isolation), tampering or energy theft. Third-party providers must ensure expected quality; establishing and monitoring strict SLAs is of paramount importance.

Security: End-to-end security is vital for most smart grid use cases that can affect stability. Privacy and availability is usually assured with asymmetric elliptic curve cryptography.

7.2.4 USE CASES AND TECHNOLOGY CONSIDERATIONS

A technology's characteristics can best be viewed in context. According to the National Institute of Standards and Technology (NIST) smart grid use cases can be grouped into six categories:

- Advanced metering infrastructure (AMI) allows utilities to collect, measure, and analyze energy consumption data for grid management, outage notification, and billing purposes via two-way communication. Examples include scheduled and on-demand meter reading.
- Demand side management implements demand response (DR) for the purpose of reducing the consumption of electric energy by customers in response to an increase in

the price of electricity. The bandwidth requirements of DR would likely be at least as high as AMI, while the requirements on the latency are stricter.

- Distributed energy resources are becoming a greater percentage of the energy supply. Reliable communications are required to monitor generation of electricity and use it effectively.
- Electric transportation holds much promise in emissions reduction and energy independence, but it also poses challenges to utilities, such as large increases in peak demand and mobility. As electric vehicles will charge at a variety of locations, it is important to maintain compatibility of communications technologies.
- Distribution automation allows utilities to monitor and control assets in the distribution network remotely (e.g. SCADA or distribution management systems) through automated decision-making, providing more effective fault detection and power restoration. This is one of the least latency-tolerant use cases.
- Wide-area situational awareness allows the prevention of power supply disruption, with synchro phasor data measurements being the key enabler for real-time power grid situational awareness and control.

The first five categories can be enabled by NAN/FAN. The coverage area and data rate requirements for different use cases vary depending on the application, but typical values are 10Km and 100Kbps, respectively. Both wired and wireless communication technologies could be appropriate for NAN networks. WiMAX, LTE, 3G and 4G are good candidates as wireless communications technologies; satellite for electric transportation and distribution automation. Wired technologies such as PLC and Ethernet could be solutions for NAN too. In NAN networks either multi-hop or single hop approach can be used based on the technology deployed.

Use cases in the last category require the transmission of a large number of data points at a high frequency (i.e. sub-second scale) and their deployment concerns a vast area of tens of kilometers comprising several load dispatch centers that support high data rates and provide long coverage distance (e.g. up to 100 km). Moreover, the communication of all smart grid components including operator control center, main and renewable energy generation, transmission and distribution, is based on wide area network technologies such as WiMAX, 4G, and PLC.

Examples of desired requirements for Smart Grid use cases are show in Table 7-2.

	Advanced Metering Infrastructure	**Demand Side Management**	**Distributed Energy Resources**	**Electric Transportation**	**Distribution Automation**	**Wide-Area Situational Awareness**
Latency	2 – 15 s	>500 ms	20 ms – 15 s	2 s – 5 m	100 ms – 2 s	20 – 200 ms
Determinism	No	No	No	No	Yes	Yes
Time Synchronization	No	No	No	No	No	Yes

Reliability	98 – 99.99 %	98 – 99.99 %	98 – 99.99 %	98 – 99.99 %	99-99.999 %	99.999 – 99.9999 %
Redundancy	No	No	No	No	No	No
Mobility	No	No	No	Yes	No	No
Peak Data Rates	100 Kbps, 500 Kbps for backhaul	100 Kbps per node/device	56 Kbps	56 Kbps	100 Kbps	1500 Kbps
Battery Power	Up to 15 years	Mains powered	Mains powered	10 - 12 h	Mains powered	Mains powered
Connection Density (per 1000 m^2)	1000	1000	50	100	50	10

Table 7-2: Smart Grid use cases and their networking requirements.

Conclusions from the outlined use cases are that most of them can be covered by wireless technology or wired communication via PLC technology. As wireless technologies provide lower installation cost, more rapid deployment, higher mobility and flexibility than their wired counterparts, they are recommended in most smart grid applications.

7.2.5 Architecture and Design Considerations

Figure 7-2 presents the smart grid conceptual model, which involves seven roles: markets, operators, service providers, power generators, transmission providers, distributors and customers. The blue lines indicate the potential business relationships that could be established among those roles. The yellow dotted lines illustrate power distribution and network connectivity. Smart grid use cases have a vast variety of actors and communications paths. The roles can be owned by different entities in different markets. For instance, a mid-west United States utility may own the operations, service provider and distribution roles meanwhile a Texas based utility, due to de-regulation, owns different roles.

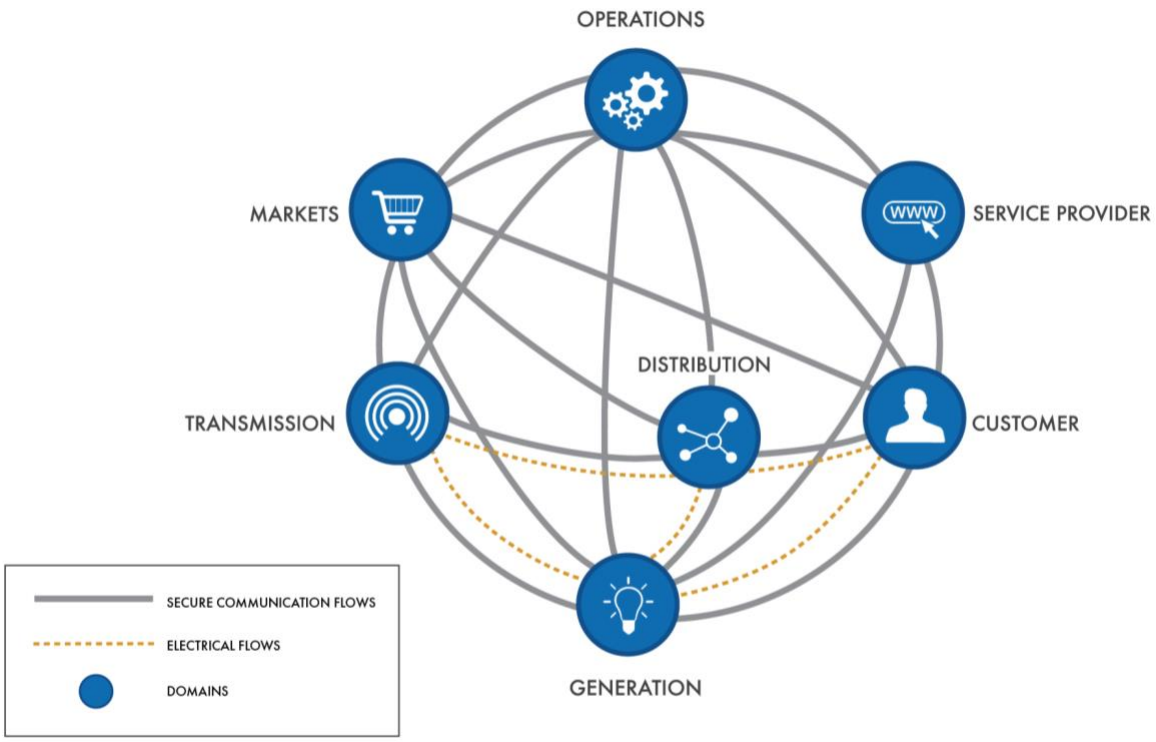

Figure 7-2: Smart grid conceptual model

Most utilities implement a two- to four-tier smart grid communication network architecture, depending on the specific applications. Each tier places different requirements on the communication network. The tiers are defined as follows and illustrated in Figure 7-3.

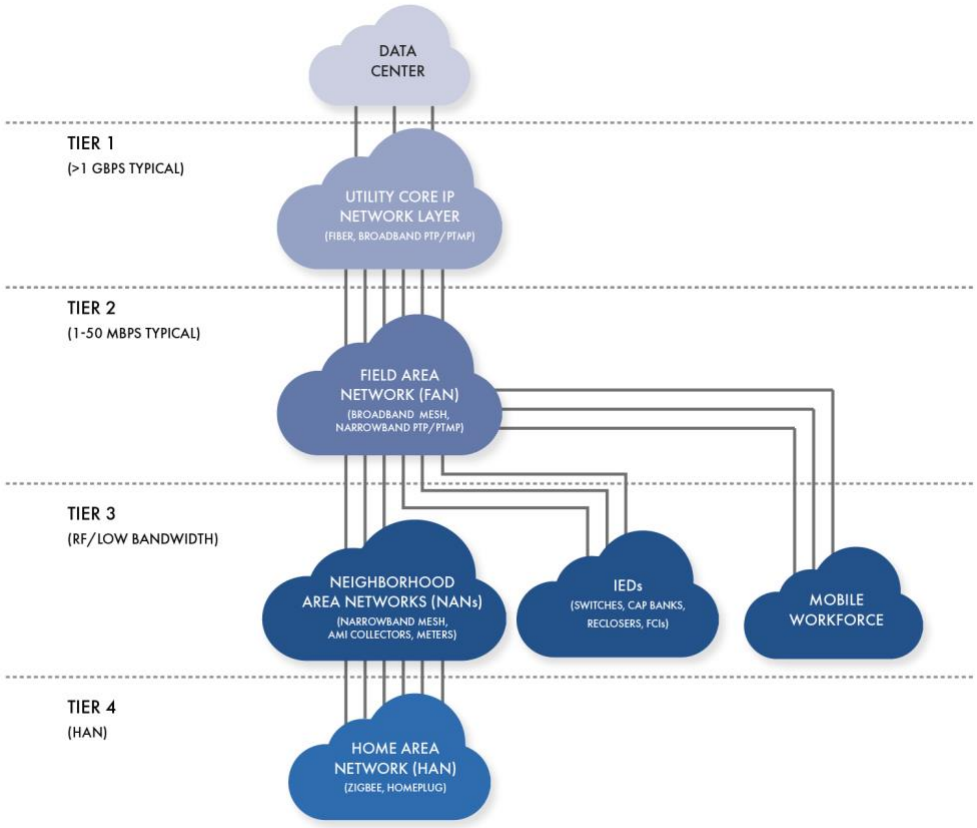

Figure 7-3: Typical utility communication network architecture

Tier 1: This is the utility's core IP network, which often connects many of its distribution substations. This tier is generally implemented with fiber. If it's economically or technically infeasible to deploy fiber, broadband PTP/PTMP is often used to extend the reach of the network.

Tier 2: The FAN fills the gap between the core Tier 1 networks, devices and personnel in the field. Substation automation devices, distribution automation devices, AMI collectors, and mobile workers equipped with laptops, tablets or handhelds connect to the FAN. FANs are generally implemented with a combination of broadband wireless mesh, narrowband PTP/PTMP and cellular data links. Endpoint connections to the FAN use wireless, wired Ethernet or serial links.

Tier 3: The NAN includes smart meters and AMI collectors. The NAN is generally implemented using narrowband wireless mesh or cellular data. When a broadband wireless mesh network is used to implement the Tier 2 network, the AMI collectors in the Tier 3 network are generally co-located with and connect to the broadband mesh routers that form the Tier 2 network. The NAN may also provide the communications interface for the Home Area Network.

Tier 4: The HAN is usually implemented using ZigBee or HomePlug technology. This provides connectivity to smart grid devices, applications and displays inside homes and businesses. If supported by the AMI system, HANs can connect to NANs via the smart meters deployed on the

customers' premises. Otherwise, the HAN connects to the utility's operations center via the internet.

7.2.6 NETWORK TECHNOLOGY RECOMMENDATIONS AND CONCLUSION

The scale of the smart grid, the wide range of demanding applications, and the paradigm shift in energy generation, pose significant challenges in the networking infrastructure. Selecting the appropriate communication technology needs careful consideration of the available options against usage requirements and business concerns, as discussed above. Besides the entire implementation complexity, a high performance, reliable and secure communication network is one of the fundamental building blocks to the introduction of smart grid applications. The key challenge in meeting this objective is to cost-effectively incorporate the necessary quantitative optimization components and capabilities into current platforms, or into a new business solution.

Conclusion for wireless network technologies in smart grid networks: Wireless technologies vary depending on the topography of where the solutions are deployed. Applications operating in HANs usually have low power consumption, low cost, and simplicity requirements, while data rates are up to 100 kbps with short coverage (up to 100 m). ZigBee, WiFi, ZWave, and Bluetooth are widely used to support such applications. At the same time, given that HANs are densely deployed in urban areas care needs to be taken to avoid interference between networks, which, for example, can result in transmission of unreliable signals from smart meters.

Applications in the NAN/FAN domain such as smart metering, demand response and distribution automation require communication technologies that support higher data rates and larger coverage. These can be implemented over ZigBee mesh networks, WiFi mesh networks, and long-distance wireless technologies, such as WiMAX and cellular. Some SCADA systems use licensed spectrum exclusively, while others use combinations of licensed and unlicensed spectrum. Unlicensed 900 MHz spectrum has been used, for example, to extend the coverage in rural areas as it is more economic than the leased spectrum alternative, while rural deployments minimize the likelihood of problems due to interference from other spectrum users. WiMAX and cellular can also be used in the WAN domain that has a very long coverage, while satellite communications can be used to provide redundant communications at critical transmission and distribution substation sites.

Conclusion for wireline network technologies in smart grid networks: Wireline technology also has a role in building smart grid networks. Particularly PLC communication can be used to reach devices that are difficult to reach with wireless technology. PLC technologies, e.g. IEEE 1901.2, are more typically deployed in Europe than North America due to having more devices per electric distribution system transformer. Along with PLC, optical communication has a role in the WAN domain, where it is commonly used as a communication medium between transmission and distribution substations and a utility control center due to its ultra-high capacity and low latency. In FANs, DSL technology is commonly deployed for residential users as it is not suitable for long distances. In general, fiber and DSL have high costs and are difficult to upgrade.

8 CONCLUSIONS AND FUTURE WORK

IoT technologies deployed in industrial settings enable the collection, transfer and analysis of data across machines and associated processes. This can significantly improve the efficiency and flexibility of industrial systems and hence foster their growth and transformation. The underlying networking technology plays a key role in meeting the business, deployment and performance requirements of applications in various industrial sectors. The selection of the right technology to use is thus a key issue that deserves careful consideration from different viewpoints. To this end, the industrial IoT networking framework presented in this document provides guidelines for the design, development, deployment and operation of successful networking solutions. This is based on a detailed analysis of stakeholder concerns from business, usage and technical perspectives, and on an elaborate overview of available networking technologies and standards. The proposed framework is use-case driven, as evidenced by the wide range of industrial IoT scenarios considered, from which network related requirements are extracted. Together with stakeholder concerns, these are used to determine the mapping of the appropriate network technology to a particular industry sector or vertical.

Part of our future work will include liaisons with standards development organizations such as the ITU-T and the IETF to receive updates on new protocols and technologies being developed, which can drive revisions to the networking framework. Examples beyond the technologies and associated features described in Section 6 include resource partitioning and isolation mechanisms (slicing and MPLS) for enabling QoS over shared network infrastructures, firewalling and demilitarized zone establishment for dependable and secure communications, as well as developments in the area of softwarized networks (SDN and NFV). In addition, we plan to set up collaborations with verticals for the purpose of promoting the proposed framework but also to acquire feedback on the use case examples provided in the last section. Such feedback will be used to improve the blueprints and to extend their applicability beyond the use cases considered. It is our wish that the IINF can be useful to various stakeholders in the industrial IoT domain, and the proposed framework can be consulted to determine the right networking technologies according to the application sector and the business needs.

Part I: Annexes

Annex A REFERENCES

[3GPP-TR37.910] Study on Self Evaluation Towards IMT-2020 Submission, 3GPP, October 2019, accessed 7 April 2021: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3190

[5G-ACIA] 5G Non-Public Networks for Industrial Scenarios, 5G-ACIA, March 2019, accessed 10 April 2019: *https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios.pdf*

[5G-CON] 5G for Connected Industries and Automation, 5G-ACIA, February 2019, accessed 04 March 2021: https://www.5g-acia.org/publications/5g-for-connected-industries-and-automation-white-paper/

[5G-TSN] 5G-TSN integration meets networking requirements for Industrial automation, Ericsson Technology Review 27 August, 2019. *https://www.ericsson.com/4a4cb4/assets/local/publications/ericsson-technology-review/docs/2019/5g-tsn-integration-for-industrial-automation.pdf*

[IETF-RFC1122] Requirements for Internet Hosts – Communication Layers, IETF STD3 RFC1122, October 1989, *https://www.rfc-editor.org/info/rfc1122*

[IIC-DDIM] Characteristics of IIoT Information Models, IIC Best Practices White Paper, accessed 24 February 2021: *https://www.iiconsortium.org/pdf/Characteristics-of-IIoT-Information-Models.pdf*

[IIC-DX] Digital Transformation in Industry, IIC White Paper, 2020 v1.0

[IIC-IICF] Industrial Internet Connectivity Framework, v1.0, 2018, *https://www.iiconsortium.org/pdf/IIC_PUB_G5_V1.01_PB_20180228.pdf*

[IIC-IIRA] The Industrial Internet of Things Volume G1: Reference Architecture, Version 1.9, IIC 2019, accessed 23 September 2020: *http://www.iiconsortium.org/IIRA.htm*

[IIC-IISF] Industrial Internet of Things Volume G4: Security Framework, IIC:PUB:G4:V1.0:PB:20160928, accessed 24 September 2020: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

[ISO/IEC7498] Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1:1994

[ITU-R M.2083] ITU-R, "IMT Vision – Framework and overall objectives of the future deployment of IMT for 2020 and beyond," accessed 23 September 2020: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

[ITU-R M.2410] ITU-R, "Minimum requirements related to technical performance for IMT-2020 radio interface(s)," November 2017, accessed 19 June 2020: *https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf*

[UCA-NET] Utilities Communications Association, "Smart Grid Networks System Requirements Specification, Release Version 5," November 2012, accessed 08 December 2020: *https://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Latest_Release_Deliverables/SG%20Network%20SRS%20Version%20V5%20Final.pdf*

[UCA-PATH] Utilities Communications Association, "Possible paths for network communications in the smart grid," accessed 08 December 2020: *https://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Latest_Release_Deliverables/Diagrams/SG-NET-diagram-r5.1D-with-Xflows.pdf*

[UCA-SEC] Utilities Communications Association, "Latency and security requirements," accessed 08 December 2020: *https://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Latest_Release_Deliverables/SG%20Network%20System%20Requirements%20Specification%20v5.1.xls*

Annex B ACKNOWLEDGEMENTS

This document is a work product of the Industrial Internet Consortium Networking Task Group, co-chaired by David Lou (Huawei) and Jan Höller (Ericsson).

Editors : David Lou (Huawei), Jan Höller (Ericsson).

Authors: The following persons have written substantial portion of material content in this document: David Lou (Huawei), Jan Höller (Ericsson), Dhruvin Patel (Ericsson), Ulrich Graf (Huawei), Matthew Gillmore (Itron).

Contributors: The following persons have contributed to this document: Otthein Herzog (TZI), Marinos Charalambides (Huawei), Konrad Nieradka (KLEO Connect), Atte Länsisalmi (Nokia), Clifford Whitehead (Rockwell Automation), Daisy Su (Nokia), Michael Hilgner (TE Connectivity), Balazs Varga (Ericsson), Janos Farkas (Ericsson), Peng Liu (China Mobile), Nampuraja Enose (Infosys), Hengsheng Zhang (CAICT).

Technical Editors: Stephen Mellor (IIC staff) and Michael Linehan (IIC staff) oversaw the process of organizing the contributions of the Authors and Contributors into an integrated document.
