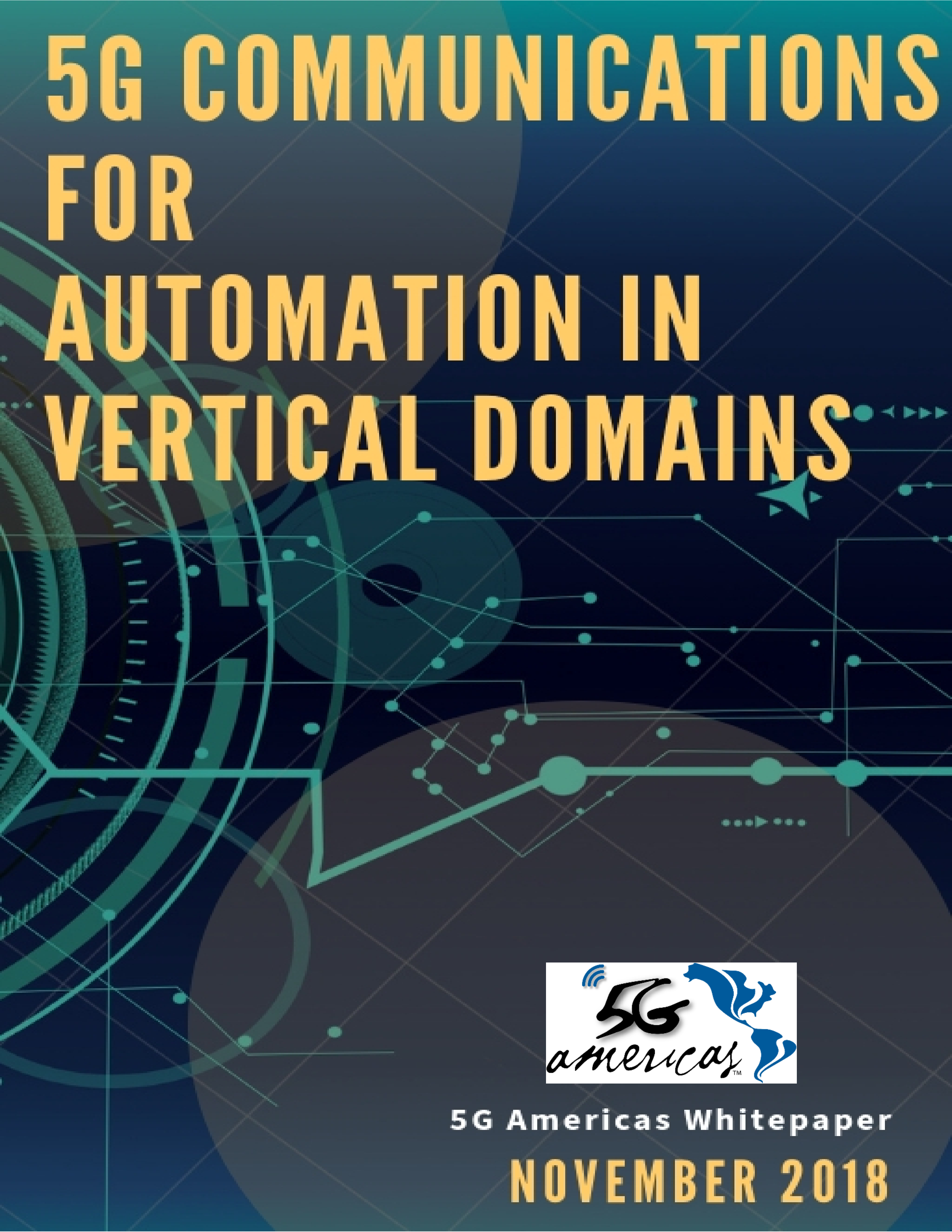
5G COMMUNICATIONS FOR AUTOMATION IN VERTICAL DOMAINS



5G Americas Whitepaper

NOVEMBER 2018

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

1. INTRODUCTION

To produce goods and deliver services in the physical world, special communications are needed. These communications often necessitate low latency, high reliability, and high communication service availability. The upcoming 5G systems are targeted to extend mobile communication services beyond mobile telephony and broadband into new vertical domains with special communication services to provide automation for various use cases and services. Key vertical domains and associated uses cases with a compelling need for automation include the following:

- Rail-bound mass transit
- Building automation
- Factory of the future
- eHealth
- Smart city
- Electrical power distribution
- Central power generation
- Program making and special events

Communications for automation in vertical domains come with demanding and diverse requirements with respect to latency, data rates, availability, reliability, and in some cases, high-accuracy positioning. Communications in this sphere must support applications for production in the corresponding vertical domain (for example, industrial automation and energy automation, but also transportation). This needs to be incorporated into new security standards and mechanisms for dependable communications.

The 3GPP standards organization has analyzed vertical use cases that resulted in several vertical communication requirements. The well-understood Key Performance Indicators (KPIs) for latency, jitter, reliability, communication service availability, and data rate apply for verticals, as well. In addition, there are other requirements that should be considered and folded into the potential new service requirements for 5G systems.

This whitepaper details the automation concepts and communication modeling in the vertical domains, mainly to foster a common understanding. It also provides an analysis of deployments with automation, discusses the requirements, illustrates security mechanisms in these domains, and identifies potential new 5G security requirements. The whitepaper further addresses key representative use cases for communication in automation in vertical domains.

A new 3GPP SA1 [1] study item on requirements for automation in verticals focuses on critical communications as an enabler for wireless control loops. Once complete, the group will have identified the normative 3GPP work needed to deliver 5G for automation in a variety of industries.

1.1 OVERVIEW OF AUTOMATION IN VERTICAL SEGMENTS

5G systems will extend mobile communication services beyond mobile telephony, mobile broadband, and massive machine-type communication into new application domains, so-called vertical domains, with special requirements toward communication services. Communication for automation in vertical domains comes with demanding requirements—high availability, high reliability, low latency, and, in some cases, high-accuracy positioning.

[1] http://www.3gpp.org/specifications-groups/sa-plenary/sa1-services.

An additional challenge is that this communication for automation must support the applications for production in the corresponding vertical domain (for instance, industrial automation and energy automation, but also transportation). This focus—together with regulations specific to vertical domains—has led to tailored communication concepts such as dependable communication and specific security standards and mechanisms. An overview of these concepts follows:

Automation refers to the control of processes, devices, or systems in vertical domains by automatic means reducing human interaction. A process always includes physical entities and their attributes and involves providing input to generate a particular output. For example, heat might be an input to a process of chemical reaction in a gas. The resulting chemical products would be the output.

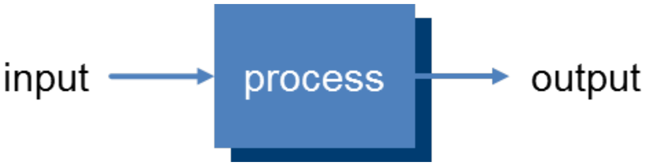


Figure 1.1. A Basic Process.

Automation is about controlling processes with the aid of automated means. This objective is accomplished using control systems. A control system is an interconnection of components forming a system configuration that will provide a desired process response.

The four key distinguishable control functions are the following:

1. Measure – measure the values from the sensors
2. Compare – evaluate the measured values relative to process design values
3. Compute – evaluate the divergence of output from the desired
4. Correct – adjust the process to achieve the desired output

These four functions are typically performed by four elements:

1. Sensor – device capable of measuring various physical properties
2. Transmitter – device that converts measurements from a sensor and sends the signal
3. Controller – provides the logic and control instructions for the process
4. Actuator – changes the state of the environment (here, the process)

The combination of sensor and transmitter is typically referred to as a sensor.

There are three common patterns of automation. The first is open-loop control. The second is feedback or closed-loop control, and the third is sequence control.[2] Open-loop control is characterized by the lack of output control where the desired output responses to an actuator are predetermined to be within an acceptable range. Figure 1.2 depicts an open-loop control system.

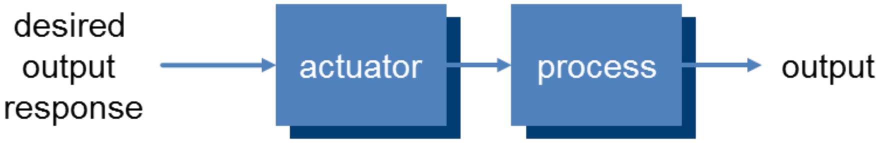


Figure 1.2. Open-Loop Control System.

[2] 3GPP TR22.804 V16, *Study on Communication for Automation in Vertical Domains*.

Closed-loop control, on the other hand, enables the manipulation of processes—even if the environment influences the process or the performance of the actuator changes over time. This type of control is realized by sensing the process output and feeding these measurements back into a controller. Figure 1.3 depicts a closed-loop control system.

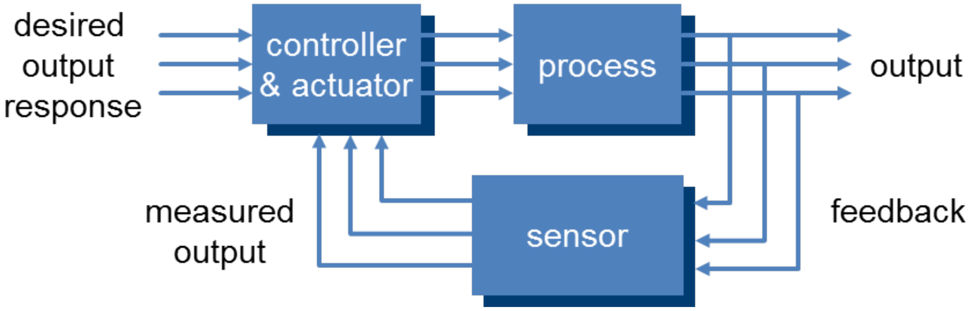


Figure 1.3. Closed-Loop Control System.

In sequence control, the actions involve either stepping through a fixed sequence or using a certain logic to conduct different actions based on various system states and system input. Sequence control is an extension of both open-loop and closed-loop control in which, instead of achieving a single output instance, an entire sequence of output instances is derived. An elevator traveling from one floor to another provides a good example of sequence control—different control actions direct the elevator from its original location to its destination.

The development of 5G technologies will enhance broadband capabilities of mobile networks. In addition, it will provide advanced wireless connectivity for automation in a variety of vertical industries, such as the manufacturing, automotive and agricultural sectors. 5G, as it is broadly understood, supports three essential types of communication: enhanced Mobile Broadband (eMBB), Massive Machine-Type Communication (mMTC), and Ultra-Reliable Low-Latency Communications (URLLC).

eMBB provides extremely high data rates and offers enhanced coverage compared to 4G. mMTC is designed to provide ubiquitous connectivity for hundreds of thousands of IoT devices per square kilometer, with wider area coverage and deeper indoor penetration. URLLC is a key feature for highly critical applications—designed to meet demanding end-to-end (E2E) latency, reliability and availability requirements for applications in automation in vertical domains.

“Industry 4.0,” the next era in industrial production, is targeting major improvements in future smart factories that include enhanced flexibility, versatility, usability and efficiency. Meeting these objectives depends on 5G features and performance.

Essential to the Industry 4.0 vision for industrial manufacturing—and to delivering seamless integration across all automation layers—are the integration of Internet of Things (IoT) and related services and features such as a peak data rate of 1–20 Gb/s; connection density 1 thousand – 1 million devices/km2; reliability of 99.999 percent; enhanced battery life of 10 years; higher position accuracy; latency 1–10 ms; and strong privacy and security.

This white paper provides an overview of the use cases where automation is targeted and identifies requirements of the vertical domain. The white paper is organized as follows:

- Section 2 discusses some of the emerging market drivers and offers a window into the use cases.

- Section 3 provides a summary of requirements. In addition, this paper discusses the key enablers—the main building blocks and features— of 5G.
- Section 4 outlines these key elements of automation, the 5G technology features and the main enablers of communications in vertical domains.
- Section 5 discusses the supporting 5G network architecture and the upper layer protocols for sample use cases.
- Section 6 highlights the issues surrounding security for communications for automation and the needed design requirements.
- Lastly, section 7 provides an update of the effort in development of the standards- in studying requirements and developing specifications that are currently underway in 3GPP.

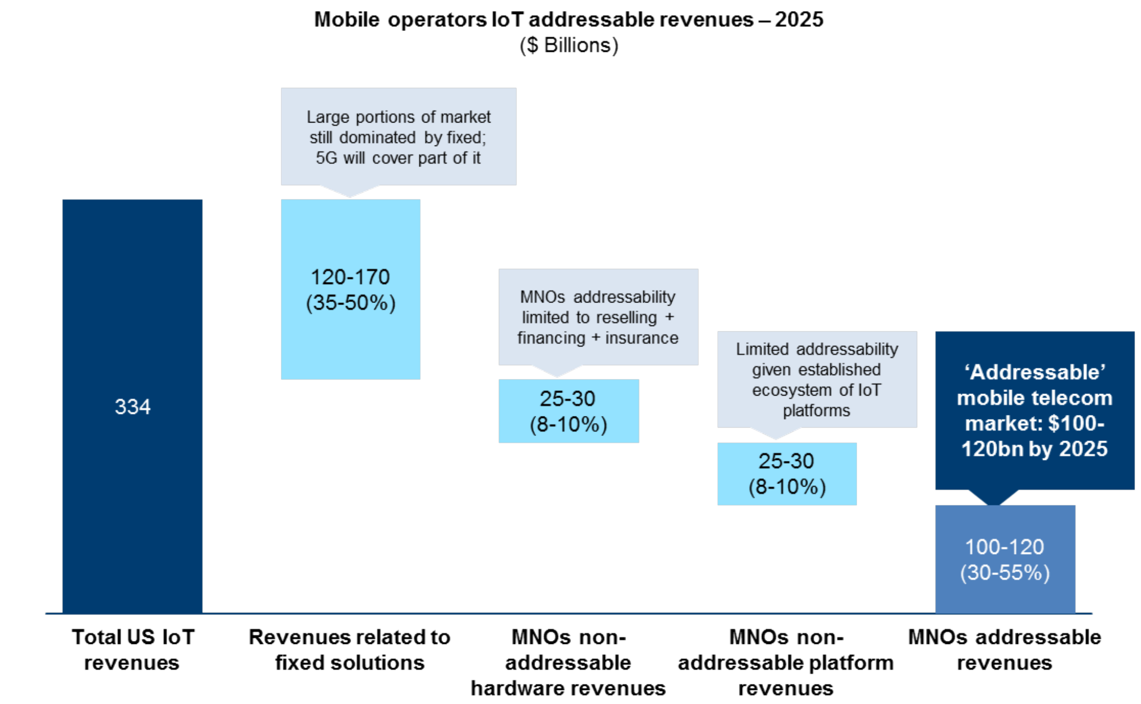
2. MARKET DRIVERS FOR AUTOMATION & KEY VERTICAL SEGMENTS

Market segments for automation are still emerging and are expected to ignite growth within the next 18-36 months. Industry is at an inflection point and will move forward with the following key objectives in mind:

- NB-IoT technologies will help drive lower costs
- 5G will enable a new range of opportunities
- New technologies such as blockchain, Artificial Intelligence (AI) and Multi-Access Edge Computing (MEC) will overcome technology limitations
- Ecosystem players will move toward more collaborative approaches

According to industry research, mobile operators' addressable revenues in the U.S. will make up $100-$120 billion or 30-35 percent, of total IoT revenues by 2025.[3] These revenues exclude 5G-related fixed solutions, non-addressable hardware revenues and non-addressable platform revenues, as illustrated in Figure 2.1.

[3] *Mobile Operators IoT addressable revenues -2025*, Delta Partners, Business Case. June 2016.

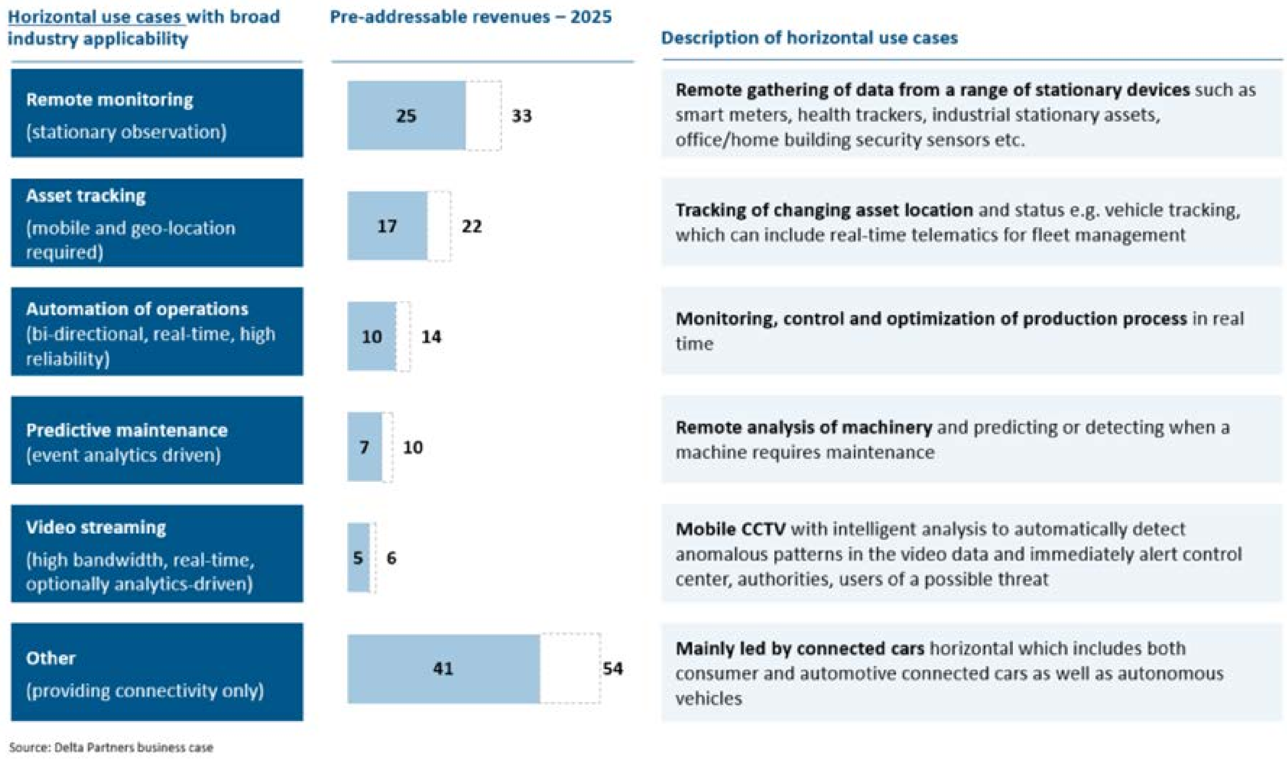


Source: Delta Partners business case

Figure 2.1. Total IoT Revenues in the U.S. by 2025.

The early value of two-way communication towards automation is likely to be concentrated in a few horizontal use cases such as remote monitoring, asset tracking, monitoring operations, preventive maintenance and video streaming; and etcetera. Delta Partners projects that the addressable revenues from these five use cases as Mobile Network Operators (MNOs) represent approximately 65 percent of the B2B (business to business) and consumer market opportunities.

As Figure 2.2 illustrates, remote monitoring represents the top horizontal use case opportunity with $25-$33 billion of the projected 2025 $100-120 billion mobile telecom market addressable revenue total. Remote monitoring is followed by asset tracking with $17-22 billion, automation with $10-14 billion, predictive maintenance with $7-10 billion and video streaming with $5-6 billion.



Horizontal use cases with broad industry applicability	Pre-addressable revenues – 2025	Description of horizontal use cases
Remote monitoring (stationary observation)	25 33	**Remote gathering of data from a range of stationary devices** such as smart meters, health trackers, industrial stationary assets, office/home building security sensors etc.
Asset tracking (mobile and geo-location required)	17 22	**Tracking of changing asset location** and status e.g. vehicle tracking, which can include real-time telematics for fleet management
Automation of operations (bi-directional, real-time, high reliability)	10 14	**Monitoring, control and optimization of production process** in real time
Predictive maintenance (event analytics driven)	7 10	**Remote analysis of machinery** and predicting or detecting when a machine requires maintenance
Video streaming (high bandwidth, real-time, optionally analytics-driven)	5 6	**Mobile CCTV** with intelligent analysis to automatically detect anomalous patterns in the video data and immediately alert control center, authorities, users of a possible threat
Other (providing connectivity only)	41 54	**Mainly led by connected cars** horizontal which includes both consumer and automotive connected cars as well as autonomous vehicles

Source: Delta Partners business case

Figure 2.2. Top Five Use Cases for B2B and Consumer Opportunities – 2025.

The top five horizontal use cases could be matched to broad industry applicability as follows:

Remote Monitoring

- Utilities – Electricity, water monitoring
- Healthcare – Remote patient monitoring
- Consumer – Alarms, security sensors and m-health

Asset Tracking

- Transport – Fleet management and monitoring
- Consumer – Asset tracking
- Automotive – Fleet management and recovery of stolen vehicles
- Manufacturing – Retail/warehouse operations

Automation of Operations

- Manufacturing – Real-time automation
- Healthcare – Remote surgery, automated robotics
- Commercial real estate – Facility automation
- Construction, oil & gas, mining – Machinery automation

Predictive Maintenance

- Automotive, transportation – Vehicle repairs, battery replacement
- Manufacturing – Equipment maintenance
- Commercial real estate – HVAC, heaters, lightning, maintenance

Video Streaming

- Consumer – CCTV cameras
- Commercial real estate – Smart security cameras

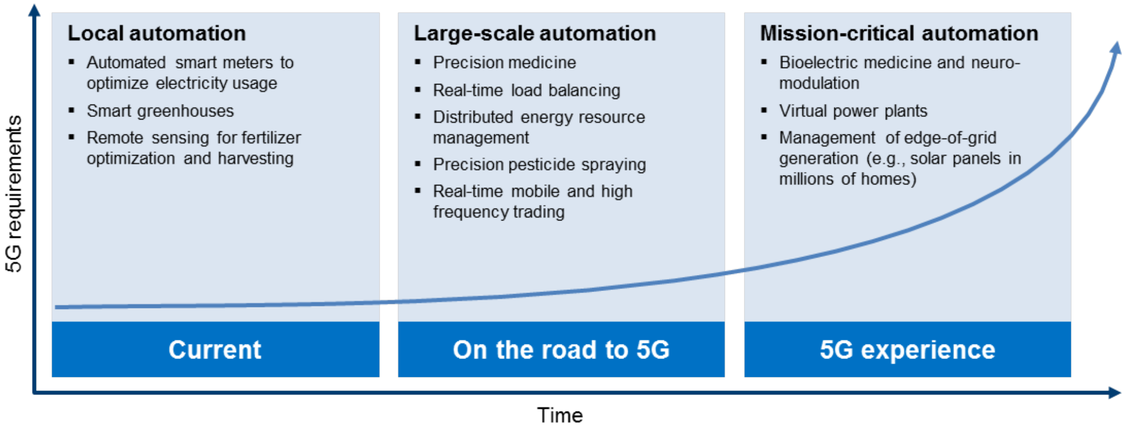
Others

- Transportation & automotive – Autonomous vehicles
- Consumer & automotive – Connected cars, connected appliances
- Retail – Real-time, in-store promotions

As we move towards 5G, real-time automation scales out from local compute to distributed large-scale compute to mission-critical experience.

In Figure 2.3, Ericsson describes the 5G evolution of real-time automation:

- Local automation such as smart meters, smart greenhouses and agricultural remote sensing
- Large-scale automation such as precision medicine, real-time load balancing, distributed energy management and real-time mobile and high frequency trading, and
- Mission-critical automation such as bio-electronic medicine, virtual power plants and management of solar grid generation, and etcetera.


Local automation
Automated smart meters to optimize electricity usage
Smart greenhouses
Remote sensing for fertilizer optimization and harvesting
Large-scale automation
Precision medicine
Real-time load balancing
Distributed energy resource management
Precision pesticide spraying
Real-time mobile and high frequency trading
Mission-critical automation
Bioelectric medicine and neuro-modulation
Virtual power plants
Management of edge-of-grid generation (e.g., solar panels in millions of homes)
5G requirements
Current
On the road to 5G
5G experience
Time

Source: Ericsson and Arthur D. Little analysis

Figure 2.3. Evolution of 5G Real-Time Automation Cluster.

Noting that vertical segments are also a good representation into enterprise, public sector or consumer sectors, the following sections describe different vertical use cases of automation and how the technology will help drive customer experience, business productivity and cost savings. An exhaustive review of a large number of use cases and associated requirements is beyond the scope of this whitepaper. Several representative examples are provided.

2.1 RAIL-BOUND MASS TRANSIT

Automation in public transport, especially in mass transit, is one of most demanding infrastructure applications. The number of driverless metro lines worldwide, which already exceeds 100, continues to grow. Enhanced communication networks and technologies are required to address some of the key challenges mass transit operators are facing today, including the following:

- Growing traffic (passenger flow, the number and frequency of mass transit vehicles)

- Passenger safety and security
- Enhanced travel comfort (for example, delivery of real-time multimedia information and access to the Internet, both in stations and on trains)

There are several main drivers behind the growing importance of communication services in mass transit:

- Passenger information
- Internet access
- Train automation

Automation of trains can be divided into control and operations that consist of distributed applications and rely on dependable communication. Control applications are considered higher priority than operational applications, and operations are higher priority than passenger services.

The main challenge is to ensure premium priority of control-related communication over other types of communication, especially since the data bandwidth consumed for control is typically overpowered by data traffic arising from the other two applications. Another important challenge is to provide superior priority of operational data communication over passenger-related communication.

2.2 BUILDING AND FACILITIES

Buildings and facilities are a major vertical segment in which automation plays a critical role in the management of equipment. Automated management of heaters, coolers, and ventilators, for example, enables reduced energy consumption, increased savings, and improved handling of repair and maintenance issues to enhance the comfort of people using the facilities.

Sensors installed in a building provide the measurements of the current environment to a Building Management System (BMS) via local controller where sensor measurements, in response, issue a command to an actuator to take desired steps as in modifying the controls (for example, a command to increase or decrease room temperature).

2.3 FACTORY OF THE FUTURE

Physical production systems based on a ubiquitous and powerful connectivity and computing infrastructure are considered to be the key enabler to achieving the primary goals of Industry 4.0, which are as follows:

- Flexibility
- Versatility
- Resource Efficiency
- Cost Efficiency
- Worker Support
- Quality of Industrial Production
- Logistics

Future smart factories are characterized by flexible, modular production systems that include mobile and versatile production assets and that require efficient wireless communication services. The vast majority of existing communication technologies used in industry are still wire-bound, using interconnecting sensors, actuators and controllers in an automation system. Wireless communications are, at the moment, primarily used for special applications and scenarios such as in the process industry or for connecting standard IT hardware to a production network or similar non-critical applications.

Previously, there was no need for wireless connectivity as production facilities were relatively static and long lasting. In addition, existing wireless technologies were not equipped to meet the demanding requirements of industrial applications, especially with respect to end-to-end latency and communication service availability.

5G wireless connectivity is expected to enable major change by providing flexibility, mobility, versatility and ergonomics which are stated as key requirements for the factories of the future—by contributing significantly to revolutionizing goods productivity, shipping and services.

2.4 eHEALTH CARE

Automation in this vertical is about transforming healthcare through mobile health delivery, personalized medicine, and social media eHealth applications. Because medical data is very sensitive and private, a high degree of reliability in transporting the data is required. 5G mobile is expected to play a significant role in advancing this aspect.

eHealth provides the capability for remote monitoring and care. This eliminates the need for frequent visits to the doctor and allows for efficient management of chronic diseases for both patients and medical professionals. This use case is about the automated monitoring of data. It suggests that such sensitive information should be managed in a secure way and, in some cases, can allow for different levels of authorization for this information.

In some cases, regular monitoring of patient data can trigger an alarm to the patient, depending on the information received. In other cases, the trigger authorizes other medical care bodies to receive other portions of the patient information, and, finally, the same information can be sent to patient and medical care bodies with different and multiple levels of authorization. Most telecare data will need to be transferred to new data management systems in order to support real-time critical alarm situations.

2.5 SMART CITY

Today, cities need delivery for a safer, cleaner and more economically vital environment to attract and retain both citizens and businesses. Cities are facing many key issues that are driving them to examine a holistic Smart Cities strategy. Among these issues are the following:

- **Increased Urbanization** – Urban populations account for 54 percent of the total global population (and they are growing)
- **Public Safety** – Recurring key issue of city leaders
- **Aging Infrastructure** – Multi-trillion-dollar effort to address
- **Economic Development** – Need for job creation and recruitment of talent
- **Environmental Sustainability** – Quality of life for citizens

A Smart City is not a single service or solution but instead covers a broad range of verticals that can support the holistic ecosystem of today's cities. Among the various verticals that can be incorporated under a 'smart cities' umbrella, along with possible solutions, are these:

- **Energy & Utilities** – Smart lighting, water management
- **Infrastructure** – Waste management, structural integrity
- **Public Safety** – Video surveillance, emergency vehicles routing
- **Transportation** – Smart parking, route optimization/traffic patterns
- **Citizen Engagement** – Municipal Wi-Fi, public transparency

The Internet of Things gives cities powerful new tools for saving money and operating more efficiently. These new, innovative, intelligent solutions build more livable cities today, as well as providing a powerful bridge to the future. Imagine that the streets and sidewalks of your city are like the nervous system in your body. At any one moment, millions of actions are taking place. There are cars racing by, people crossing the street, lights changing and sensors being tripped. Being able to capture information from intelligent nodes placed throughout a city and quantify activity is akin to putting your finger on the pulse of the city. A smart city infrastructure is the foundation to drive synergistic outcomes across multiple departments, provide a safer, cleaner city, enable new revenue streams and unleash the exponential growth of a new economy. A 5G smart city infrastructure is the future—with its ability to support a denser and more economical rollout of sensors and devices supporting higher throughput, along with longer battery life.

2.6 ELECTRICAL POWER DISTRIBUTION

The energy sector is in the process of evolution towards renewable energy with a large number of power plants based on solar, wind and other sources of power. New sensors and actuators are considered and deployed in the power system to efficiently monitor and control the volatile conditions of the grid, requiring real-time information exchange. The emerging electric-power distribution grid is referred to as Smart Grid. Smart Grid helps in improving power reliability and quality, grid resiliency, power usage optimization, operational insights, renewable integration, insight into energy usage, and safety and security. The controllability and predictability of processes drives the operation and economic performance, which are prerequisites for the sustainable and scalable integration of renewables into the grid. With the introduction of 5G in Smart Grids, it is expected that wireless connectivity can provide a higher degree of flexibility, mobility, versatility and ergonomics, and can fundamentally revolutionize how electric energy is monitored, stored, and controlled.

2.7 CENTRAL POWER GENERATION

This vertical is concerned with centralized power generation, which is the conversion of chemical energy and other forms of energy into electrical energy. Typical electric-power outputs are 100MW and more—that includes large gas turbines, steam turbines, combined-cycle power plants, wind farms, and etcetera. The planning, installation of equipment, operation, monitoring and maintenance of these plants makes up this vertical domain.

This use case covers applications that access existing local plant control systems via wireless connections. Control systems are monitored, and the information is communicated between a power unit and graphical user interfaces. The information transported to and fro conveys states of, and changes in, process parameters, control settings, and/or power unit characteristic parameters with stringent real-time requirements. Automation using 5G in this vertical domain uses low latency and connectivity features to provide compelling benefits.

3. REQUIREMENTS FOR AUTOMATION WITH 5G COMMUNICATIONS

3.1 REQUIREMENTS

The Third Generation Partnership Project (3GPP) continues to provide the necessary standardized platform for building a consensus for the requirements for automation with 5G.

3.1.1 3GPP RELEASE 15

With the recent advances in active antenna technology, it is possible for operators to significantly increase the capacity and coverage of their networks. The first phase of 5G technology, in 3GPP Release 15, includes the core architectural and protocol enhancements needed to support different kinds of User Equipment (UEs)—for example, for the IoT, services, technologies, and new deployment scenarios. In Rel-15, the focus is on flexible support of enhanced mobile broadband (eMBB) and meeting diverse sets of requirements for Ultra-Reliable and Low Latency Communication (URLLC). These cover a broad set of requirements for new functionalities such as network slicing, enhanced mobility management and multiple access technology convergence, as well as requirements for signaling and transmission efficiencies in the control plane, user plane and energy consumption.

With communications for industrial automation having long been considered a driver for 5G technology, system enhancements made to the 3GPP 5G System in Rel-15 have addressed the basic needs in support of industrial automation and have established a base for building an industrial automation communications system.

Network slicing allows a subset of network functions to be made available to a limited set of users for a specific purpose. This capability provides significant benefit for industrial automation in that a network can be subdivided to meet specific needs of different devices. For example, robots may be constrained to use a specific set of functions providing URLLC, while humans may be able to access additional functionality, including access to both the industrial network and a public network for communication services. The initial set of network slicing requirements address aspects such as these:

- Creation, modification and removal of a slice
- Ability to assign a device to and remove a device from a slice
- Ability to scale slice capacity based on various factors (for example, demand, time of day)
- Connectivity for both home and roaming devices
- Establishment of priority access and QoS (quality of service) for users of a slice
- Slice management that prevents changes in a slice (for example, scaling) and traffic in a slice (for example, congestion) from impacting other parts of the network outside of the slice

A slice can be deployed to provide a specific service or set of services for an enterprise, in which case that tenant may want to provide some of their own applications and manage the slice resources themselves. To facilitate this new style of operation, new APIs have been established to allow slice management by either the network operator or a third party.

Enhanced mobility management requirements allow for efficient support of different types of devices in an industry automation scenario. Such devices may be stationary, nomadic or have mobility only within a specific geographic area such as a factory. In these cases, the fully flexible mobility management typically provided by the 3GPP system is not only unnecessary, but it also results in signaling inefficiencies for these devices. There is no need for paging or other location tracking signaling when a device is not moving or when its range of movement can be known a priori. Rel-15 includes requirements to support efficient mobility management for these types of devices.

The introduction of 3GPP 5G technology into the industrial automation environment is likely to occur in a gradual manner. Such environments currently use a variety of communication transport mechanisms such as wires or WLANs. As 5G is introduced, the need to interwork with, and even emulate, existing communication transport mechanisms will be essential. Rel-15 requirements begin to address these needs in support of 3GPP and non-3GPP access technology convergence in the following ways:

- By specifying efficient interactions and traffic management among the different access technologies
- By requiring service continuity when changing access type
- By supporting simultaneous connectivity

IoT applications in industrial automation are key drivers for Rel-15 efficiency enhancements in both the control and user plane for 5G. While IoT is supported in earlier versions of 3GPP systems, the anticipated increase in the number and types of devices necessitates even more efficient operation. For example, sensors and tracking devices can take advantage of the mobility management efficiencies for stationary and nomadic attachment. Robots in a factory may rely on cloud-based applications to support a high data rate and low latency. Medical monitors may require efficient transmission of infrequent small amounts of data, while a street corner monitor may require the ability to efficiently stream video when an accident occurs, as well as the infrequent small data during periods of inactivity. Control plane efficiency requirements address the signaling needs for scenarios such as these. Other signaling efficiencies are proscribed for devices to discover nearby devices they need to communicate with, and for communications among a dense concentration of devices.

User plane efficiencies requirements include support for mechanisms such as mobile edge computing, where services can be redundantly located within a network such that latency and reliability can be maintained for moving devices. Requirements address aspects such as the following:

- Managing traffic distribution among service instances
- Maintaining QoS as devices move and change service instances
- Providing service continuity as a device moves and changes service instances
- Supporting both operator and third-party service instances

Specifically, for the support of mobile edge computing, the 5G system enables selection of an IP anchor node close to the network edge and offloading of IP traffic from the 5G network onto traditional IP routing networks via an IP anchor node close to the network edge. As such, the end-to-end latency can be reduced for a better user experience to accommodate different UEs with different mobility characteristics and required QoS. In view of the 5G system, the support of mobile edge computing can reduce signaling overhead and optimize access for different types of UEs.

Energy efficiency is tightly coupled with the other requirements for industrial automation where operations include many devices with various capabilities operating within the enterprise. Factory operations are expected to continue without disruption, even when the power supply is not reliable. Many IoT devices are small battery-operated mechanisms without any other continuous power supply. Rel-15 includes requirements to support these needs with energy savings for both the network and the devices.

3.1.2 3GPP RELEASE 16

Further enhancements of the 3GPP 5G system in Rel-16 will build upon the previously mentioned core areas to increase applicability of the 5G system for industrial automation in terms of cellular IoT service provisioning in the 5G system, deployment options for supporting networks for industrial automation in vertical domains, KPIs for different use cases, business role models of network slicing, 5G LAN type services and corresponding security protection mechanisms.

3GPP SA1 has completed several studies related to providing 3GPP support for automation communications. These studies are listed below:

- TR 22.804, Study on Communication for Automation in Vertical Domains
- TR 22.821, Feasibility Study on LAN Support in 5G
- TR 22.830, Business Role Models for Network Slicing

The results of the studies are now being transposed into normative requirements in TS 22.261 and, for requirements specific to communication for automation, TS 22.104. The transposition process will complete by the end of 2018.

SA2 has also initiated several studies for Rel-16 that consider the results of the three SA1 studies. The SA2 studies are listed below:

- TR 23.740 Study on Enhancement of Network Slicing
- TR 23.734 5GS Enhanced support of Vertical and LAN Services

At the time of writing, there are no conclusions from the SA2 studies.

3.2 PERFORMANCE KPIs

3.2.1 RELEASE 15

Many industrial automation applications rely on both very high reliability and very low latency for accurate communications. For example, on a factory floor, timeliness and precision are required for robotic equipment to function. All commands, controls and communications between robots, and between humans and robots, occur in a highly controlled environment. Four categories of such uses were considered in Rel-15 as the basis for establishing basic KPIs:

- Discrete automation requires high reliability and availability for communications between a restricted set of devices typically covering a limited geographic area (for example, a factory floor)
- Process automation requires high availability for communications between a restricted set of devices typically covering a limited geographic area (for example, a water distribution plant)
- Electricity distribution requires high availability for communications between many devices typically over a broad geographic area (for example, a city, county, or region)
- Intelligent transport systems require high reliability and availability as well as very low latency for communications. Devices, generally, have no relationship other than proximity. While specific communications occur within a limited geographic area, the system is expected to provide wide area coverage

The specific KPIs for these ultra-low latencies, high-reliability communications (URLLC) are in Table 3.1 from 3GPP TS 22.261, replicated below.[4]

Table 3.1. Performance Requirements for Low Latency and High Reliability.

Scenario	Max. allowed end-to-end latency (note 2)	Survival time	Communication service availability (note 3)	Reliability (note 3)	User experienced data rate	Payload size (note 4)	Traffic density (note 5)	Connection density (note 6)	Service area dimension (note 7)
Discrete automation	10 ms	0 ms	99,99%	99,99%	10 Mbps	Small to big	1 Tbps/km^2	100 000/km^2	1000 x 1000 x 30 m
Process automation – remote control	60 ms	100 ms	99,9999%	99,999%	1 Mbps up to 100 Mbps	Small to big	100 Gbps/km^2	1 000/km^2	300 x 300 x 50 m
Process automation – monitoring	60 ms	100 ms	99,9%	99,9%	1 Mbps	Small	10 Gbps/km^2	10 000/km^2	300 x 300 x 50
Electricity distribution – medium voltage	40 ms	25 ms	99,9%	99,9%	10 Mbps	Small to big	10 Gbps/km^2	1 000/km^2	100 km along power line
Electricity distribution – high voltage (note 2)	5 ms	10 ms	99,9999%	99,999%	10 Mbps	Small	100 Gbps/km^2	1 000/km^2 (note 8)	200 km along power line
Intelligent transport systems – infrastructure backhaul	30 ms	100 ms	99,9999%	99,999%	10 Mbps	Small to big	10 Gbps/km^2	1 000/km^2	2 km along a road

NOTE 1: Currently realized via wired communication lines.

NOTE 2: This is the maximum end-to-end latency allowed for the 5G system to deliver the service in the case the end-to-end latency is completely allocated to the 5G system from the UE to the Interface to Data Network.

NOTE 3: Communication service availability relates to the service interfaces, reliability relates to a given system entity. One or more retransmissions of network layer packets may take place in order to satisfy the reliability requirement.

NOTE 4: Small: payload typically ≤ 256 bytes

NOTE 5: Based on the assumption that all connected applications within the service volume require the user experienced data rate.

NOTE 6: Under the assumption of 100% 5G penetration.

NOTE 7: Estimates of maximum dimensions; the last figure is the vertical dimension.

NOTE 8: In dense urban areas.

NOTE 9: All the values in this table are targeted values and not strict requirements. Deployment configurations should be considered when considering service offerings that meet the targets.

[4] 3GPP TS 22.261 v15.5.0: *Service requirements for the 5G system.*

3.2.2 3GPP RELEASE 16

As of September 2018 (the time of the writing of this white paper), no normative performance requirements have been agreed in 3GPP. The work is planned for completion by the end of 2018.

4. 5G FEATURES & ENABLERS FOR AUTOMATION IN VERTICAL DOMAINS

Automation in vertical domains will require new mobile wireless technical capabilities that will be available in 5G. There are multiple areas considered both an evolution and revolution that will enable the mobile wireless industry to address these important new markets. This section describes some of the critical features and functionality of 5G for vertical domains.

4.1 KEY AREAS OF RADIO COMMUNICATION FOR AUTOMATION

The 5G system, shown in Figure 4.1, is built on "flexible" radio access nodes, distributed and centralized data centers allowing for flexible allocation of workloads. These nodes and data centers are connected via programmable transport networks. The transport networks are connected via backbone nodes that carry the information from the access nodes to the data centers where most of the data is stored and the network is managed. Figure 4.1 illustrates that all applications, including many network applications, are run on top of a cloud with the exception of dedicated functions in the access nodes. The applications can be centralized (App 3 and App 4) or distributed (App 1, App 2), depending on the requirements.

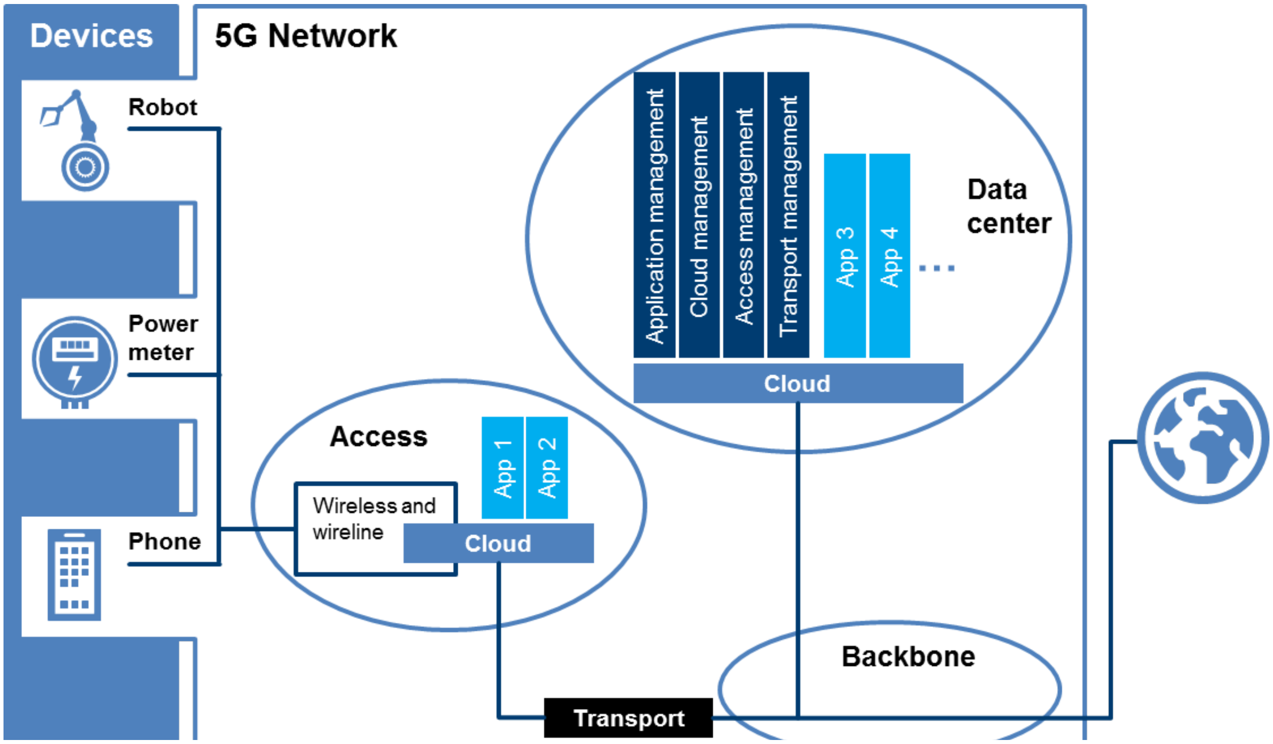


Figure 4.1. 5G Distributed System.

In addition to this, the management of applications, cloud, transport and access resources is shown centrally in the data center but can, of course, also be flexibly allocated, as necessary.

The 5G system will fully support the concept of network programmability for all types of services. A service can be flexibly allocated anywhere in the network, at a network node, end-user device or external host. A service may not be confined to an operator's network and may originate from outside the network domain.

E2E orchestration is needed to match external business offerings with network efficiency. For example, to optimize content delivery in eMBB service, orchestration would place virtualized network functions on resources that are physically close to the subscriber.

4.1.1 AUTOMATION APPLICATION

The term “automation” stands for the control of processes, devices or systems, in vertical domains, by automatic means. Rel-16 touches the main type of systems used in automation, controls systems, activity patterns in automation, communication attributes, and finally communication patterns entailed by automation systems.

As previously discussed, various studies are under way in Rel-16 to address 5G communication for automation in different vertical domains, Non-Terrestrial Networks (NTN), Vehicle-to-everything (V2X), public safety and Industrial Internet of Things (IIoT). For NTN, New Radio (NR) Release 15 will need to be modified to support satellite communications, specifically at millimeter wave (mmWave bands). For V2X, further study is proposed for dynamic support for sidelink (PC5) as well as access network (Uu) interfaces. New evaluation methodology is being defined for V2X use cases including vehicle platooning, advanced driving to enable semi-automated or fully automated driving and remote driving.

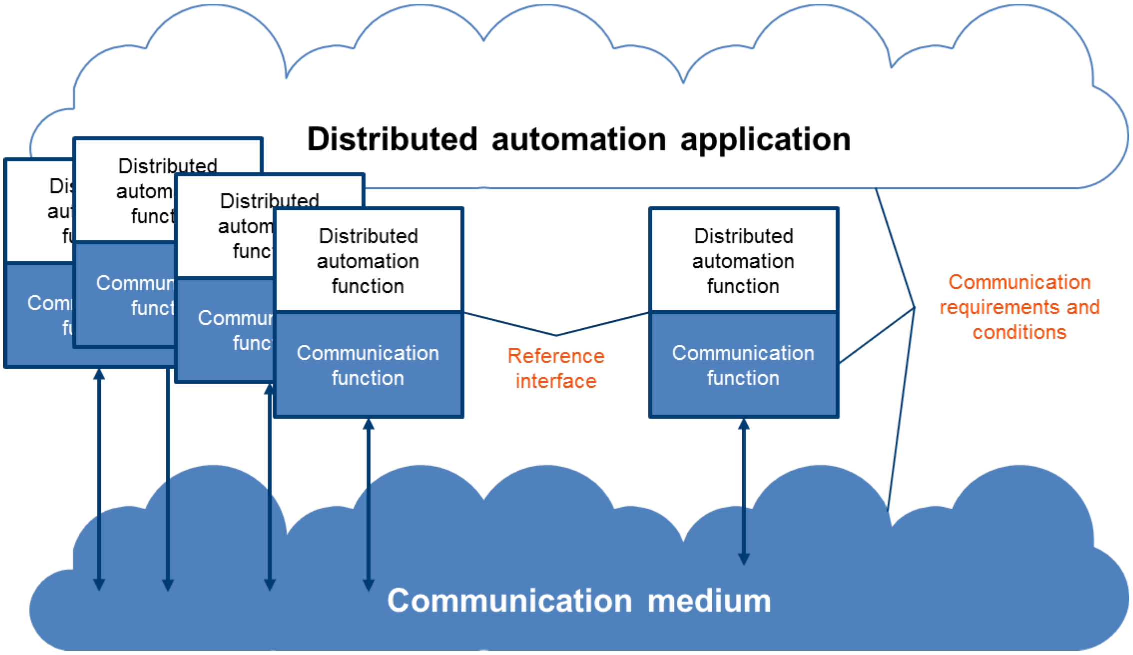

Distributed automation application
Distributed automation function
Communication function
Distributed automation function
Communication function
Reference interface
Communication requirements and conditions
Communication medium

Figure 4.2. Automation Application in a Communication System.

Rel-16 defines the modeling of communication in automation by introducing a distributed automation application system which is the aggregation of a number of automation functions. These can be functions in sensors, measurement devices, drivers, switches, I/O devices or encoders.

For the automation application system to operate, messages need to be exchanged between spatially distributed application functions. For that process, messages are exchanged at an interface between the automation application system and the communication system.

4.1.2 LOGICAL LINK

If a dependability assessment needs to be performed, it is necessary to specify an asset, its function, and the conditions under which the function is performed. The logical link is a possible asset within the area of consideration. The logical link is the link between a logical endpoint in a source device and the logical endpoint in a target device. Logical endpoints are elements of the reference interface, which may group several logical endpoints together.

4.2 OPERATIONAL AND FUNCTIONAL CONSIDERATIONS FOR AUTOMATION

Automation in vertical domain use cases presents specific operational or functional requirements in addition to performance requirements. Examples of operational requirements include demands for simple system configuration, operation, management, and assurance mechanisms such as monitoring, fault management, etc. Examples of functional requirements include aspects such as security, functional safety, authentication, identity management and etcetera.

Dependability of an item is defined as the "ability to perform as and when required, a property paramount to any automation system. A critical operational requirement for a production line to operate smoothly and faultlessly which implies that every station and component should work as intended.

Automation systems that are not dependable can, for instance, be unsafe or they can exhibit low productivity. System dependability in further defined below as this is used to analyze communication dependability and its implication for 5G systems.

Dependability is subdivided into five system properties in Figure 4.3: reliability, availability, maintainability, safety, and integrity.

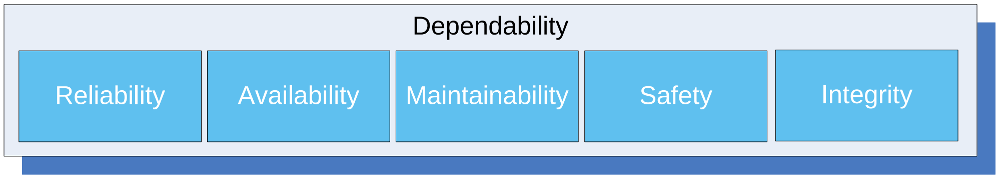


Figure 4.3. Five Facets of System Dependability.

To be suitable for automation in vertical domains, 5G systems need to be dependable. Therefore, they need to have the following system properties:

- **Reliability**: Automation functions need highly reliable communication.
- **Availability**: Availability refers to the ability to be in a state to perform as and when required, under given conditions, assuming that the necessary external resources are provided.
- **Maintainability:** Maintainability can be retained in, or restored to, a state in which it can perform as required under given conditions of use and maintenance.
- **Safety:** Safety stands for the absence of catastrophic consequences on user(s) and environment. For a distributed automation system, this implies that neither the automation functions (including

their physical embodiment), nor the processes, nor the environment should be damaged by the communication system.

- **Integrity:** Network integrity is the ability to ensure that the data throughput contents are not contaminated, corrupted, lost or altered between transmission and reception.

These properties essentially define the strength and quality of service availability, communication service continuity, communication service reliability and the probability of an erroneous message transmission. This, in turn, determines the ability to automate a given communication transaction over a logical link.

Automation in vertical domains has very high requirements for dependability, especially compared to traditional use cases in the consumer domain.

4.3 SYSTEM LEVEL ENABLERS FOR AUTOMATION

Enablers for automation began in 4G LTE (Long Term Evolution) as the mobile wireless industry continued to progress network capabilities in terms of IoT, latency and data throughput. In 5G, system-level enablers move to a new level to provide the necessary capabilities for automation.

4.3.1 MASSIVE MACHINE-TYPE COMMUNICATION (MMTC)

mMTC is designed to provide wide-area coverage and deep penetration for hundreds of thousands of devices per square kilometer. An additional objective of mMTC is to provide ubiquitous connectivity with relatively low software and hardware complexity and low-energy operation. Many of the devices supported are battery powered or driven by alternative energy supplies, have small payloads, and might rarely be active, so they tend to be relatively delay-tolerant for the most part.

While the devices typically have a long lifespan, services and software need to scale and be swapped out relatively quickly to address new business opportunities. Examples that fall into this service category include the monitoring and automation of buildings and infrastructure, smart agriculture, logistics, tracking and fleet management.

4.3.2 URLLC

The second category of application being addressed is that of cMTC (critical Machine-Type Communication), which is also called Critical IoT. In this type of application, monitoring and control occur in real time, E2E latency requirements are very low (at millisecond levels), and the need for reliability is great.

The performance objectives of cMTC will be applied to workflows such as the automation of energy distribution in a smart grid, industrial process control and sensor networking—where there are stringent requirements in terms of reliability and low latency at the application layer.

These are sometimes referred to as Ultra-Reliable Low-Latency Communications (URLLC) requirements. Careful attention will need to be paid to security in the case of both mMTC and cMTC. For more information on security in 5G and URLLC, 5G Americas has two white papers that have greater detail.[5]

[5] *The Evolution of Security in 5G*, 5G Americas and *New Services & Applications in 5G Ultra-Reliable Low Latency Communications*, 5G Americas. November 2018.

While higher network and device complexity is more readily acceptable in critical communication, mMTC will have to address cyber-security assurance with low-complexity devices. A hierarchical approach to the network is necessary to progressively improve security so that end-to-end security assurance can be guaranteed.

4.3.3 ENHANCED MOBILE BROADBAND

Providing both extreme high data-rate and low-latency communications, enhanced mobile broadband (eMBB) also offers extreme coverage—well beyond that provided by 4G. Connectivity and bandwidth are more uniform over the coverage area, and performance degrades gradually as the number of users increases. For eMBB, 5G will support peak rates of 20 Gb/s in the downlink and 10 Gb/s in the uplink. High data rates in 5G are mainly enabled by a wide system bandwidth (up to 400 MHz) and employing massive MIMO using a large number of antennas and high modulation orders, such as 256 Quadrature Amplitude Modulation (QAM). 5G operations are planned for carrier frequencies from below 1 GHz up to 86 GHz and in both the licensed and license-exempt spectrum.

4.3.4 NETWORK SLICING

Network slicing support, in a 5G system in Rel-15, is described in TS 23.501.[6] The Public Land Mobile Network (PLMN) defines a network slice which can include the Core Network Control Plane and User Plane Network Functions, Next Generation Radio Access Network (NG-RAN) for 3GPP access, and the interworking function with the non-3GPP Access Network for non-3GPP (N3GPP) access. As such, a single UE may be served by one or more network slice instances simultaneously via a 5G system, regardless of the access type(s) over which the UE is registered (therefore, 3GPP Access and/or N3GPP Access).

Each network slice may support different features and have different network function optimizations. Each network slice can be identified by a network slice identifier, which is composed of a Slice/Service Type (SST) referring to the expected network slice features and services and optional slice differentiators referring to the complemented information for the same SST. For example, the operator can deploy multiple network slice instances delivering the same features but for different groups of UEs located in a specific geographical area and dedicated to a specific customer (for example, a power company). Such network slices may have different network slice identifiers with the same Service Type but different slice differentiators.

To ensure global interoperability for network slicing so that PLMNs can support roaming more efficiently, 3GPP has provided some standardized Slice/Service Types (SST) with corresponding values, including SST value 1 for eMBB, SST value 2 for URLLC and SST value 3 for MIoT (Massive IoT).

In Rel-16, to further support the varying deployment options for industrial automation communications in a vertical domain (for example, using a private slice deployment for the sole use by a specific tenant), 3GPP SA1 Working Group (WG) has studied the following aspects and has identified corresponding service requirements for 5G system enhancements:

- Different business role models for network slicing and corresponding network slice characteristics (for example, slice scalability and flexibility)
- Trust and security relationships between MNOs and slice tenants under various business role models

[6] 3GPP TS 23.501, System Architecture for the 5G System. 2017.

4.3.5 MULTI-ACCESS EDGE COMPUTING (MEC)

MEC is a network architecture concept that enables cloud computing capabilities and an IT service environment at the edge of any network. MEC essentially provides IT and cloud-computing capabilities within the Radio Access Network (RAN) near mobile subscribers. By running applications and performing related processing tasks closer to the user, MEC helps reduce the network congestion.[7] It is also important to note how edge computing is being used and understood. A specific working group called MEC does exist in the European Telecommunications Standards Institute (ETSI), however MEC is more often referred to as a general term for edge computing.

MEC enables flexible deployment of new applications and services for customers and allows operators to provide RAN access to authorized third parties, such as application developers and content providers by implementing near the cellular base stations or other edge nodes.

Instead of sending all data to a cloud for processing, the network edge analyzes, processes, and stores. Thus, MEC can provide a means to move processing from a centralized cloud to the edge of the network or closer to the automation function.

For application developers and content providers, MEC provides a service environment with low latency and high bandwidth, as well as direct access to real-time radio network information, such as subscriber location, cell load, and etcetera that can be used by applications and services to offer context-related services.

Automation in vertical domains can greatly benefit from this MEC feature, as this allows content, services and applications to be accelerated, increasing responsiveness from the edge. The automation functions can be efficiently implemented in the network and service operations, based on insight into the radio and network conditions.

5. UPPER LAYER DESIGN AND NETWORK ARCHITECTURE FOR 5G AUTOMATION

As part of 5G specification and systems development, 3GPP has analyzed several vertical use cases which have resulted in several vertical communication requirements including high availability, high reliability, low latency, and in some cases, high-accuracy positioning for 5G systems. The application layer software for these systems supporting communication for automation in vertical domains may be developed using OSS (Operational Support Systems) and BSS (Business Support Systems) frameworks.

From a network architecture perspective, these applications can be supported by private networks, which may or may not interact with an external network managed by a 3GPP operator. To ensure feedback control, monitoring interfaces are required, as well as multi-tenancy to ensure operation by multiple users.

5.1 NETWORK ARCHITECTURE

The 5G network architecture for supporting communication for automation in vertical domains may be based on non-public networks. A non-public network is a 3GPP network where agreements between the network operators, service continuity, and roaming between a non-public network and PLMN exist. Non-public networks may be found in specialized environments such as in a factory or plant, in an enterprise, in

[7] *Mobile Edge Computing Introductory Technical White Paper*, etsi.org. October 2015.

an agricultural setting, or other such environment. 5G systems will support the capability to deploy these networks in either licensed or unlicensed bands.

Non-public networks can support network access using identities, credentials and authentication methods provided and managed by a third party and supported by 3GPP. A non-public network may be deployed in a configuration where it is a subset of a PLMN. In such cases, the PLMN will expose suitable APIs to allow an authorized third party, therefore, the non-public network tenant, to define and reconfigure the properties of exposed 5G communication services.

To better understand the network architecture for different applications in vertical domains, a few use cases are provided that will give a better idea of system and network requirements and challenges imposed on 5G systems by communication for automation.

5.1.1 USE CASE 1: REMOTE CCTV MONITORING IN SMART CITY

The smart city use case involves data collection and processing to efficiently monitor and control city resources. One use case where this is evident is in analysis of CCTV streams for enforcing restricted zones at various related retail locations across a city. The camera may be positioned and configured to monitor an emergency fire escape and door and could implement motion detection. On detecting motion in its field of view, the camera live streams the video to a video analytics server via a 5G Mobile Network Operator (MNO) network.

The video analytics server performs object and facial recognition to determine that this is not a threat. It alerts the on-site operators of the retail venue of the situation and includes advice to cancel any ongoing alarms in that area. An example of the deployment scenario is shown in Figure 5.1.

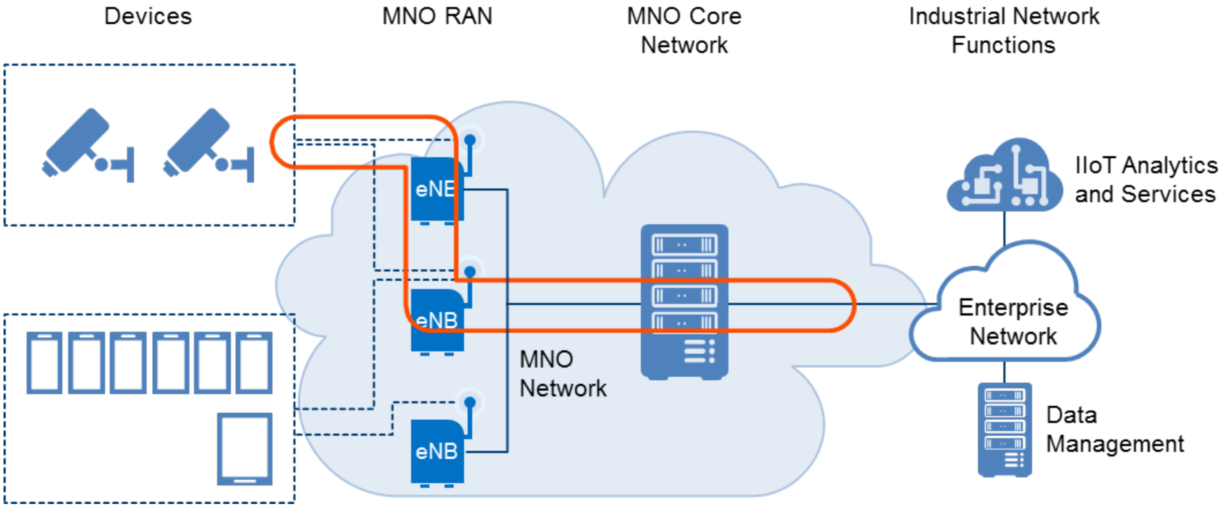


Figure 5.1. Smart City: Remote CCTV Analysis.

The network architecture in this case consists of a non-public network that interacts with a PLMN-based network of an MNO to send the CCTV video stream to a dedicated video analytics server. A dedicated network slice is used in this scenario to ensure that the video streams have enough guaranteed quality of service to remain at a high quality, consistent latency and throughput to prevent buffering.

5.1.2 USE CASE 2: FACTORIES OF FUTURE

An industrial automation application is a complex system that encompasses many hardware and software products of different types and from different vendors. Industrial automation systems are locally distributed and are typically served by wired and wireless communication networks of different types and with different characteristics. If the production process—or one of its sub-processes—does not work properly, there is the need to quickly find and eliminate the related error or fault to avoid significant production and, thus, financial losses. To that end, automation devices and applications implement diagnosis and error-analysis algorithms as well as predictive maintenance features.

5.1.2.1 CONNECTIVITY FOR THE FACTORY FLOOR

A factory floor has adopted 5G networks for wireless automation, where a variety of sensors, devices, machines, robots, actuators and terminals are communicating to coordinate and share data. Some of these devices may be directly connected to a local non-public network and some may be connected via gateway(s).

Operators, technicians and engineers have 5G enabled devices. These devices have subscription information to access the local network. These devices may also have subscription information for other networks.

Factory equipment and human operators and technicians have enough connectivity and credentials to connect to the local network, authenticating with the local core network. Typical closed-loop control applications run over this network with extremely low latency and high reliability. Due to the dedicated nature of the network, there is also high availability and consistency of latency and throughput.

In the case of a device which does not have subscription information for the network, the local core network will reject the attempt, resulting in the local Radio Access Network (RAN) refusing access to the device.

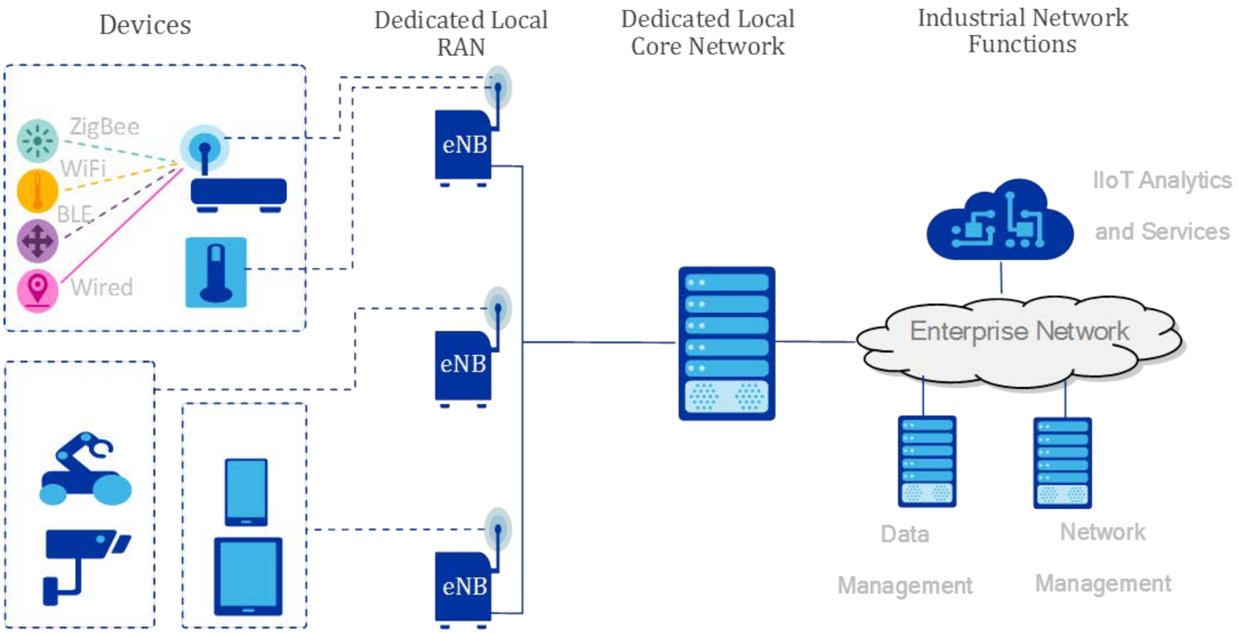


Figure 5.2. Factory of the Future with a Private Network.

Technicians can access the network on site and ensure high availability due to preemptive maintenance for the local network. Network optimization can also be performed with a higher level of aptitude due to tighter integration with the process control. In the case of catastrophic failure, technicians can repair the network on site. Devices can be onboarded directly by the factory owner. The potential post conditions are typically closed-loop control applications operating with consistent and appropriate performance.

5.1.3 USE CASE 3: WIDE AREA CONNECTIVITY FOR FLEET MAINTENANCE

An example of wide-area connectivity for fleet maintenance deployment scenario would be a Heavy Goods Vehicle (HGV) manufacturer with an ongoing contract with a haulage company to constantly track the performance of a fleet of vehicles and automatically remap their Electronic Control Unit Over-the-Air (OTA) to ensure efficient performance based on haulage load. In this scenario, wide area coverage is essential, and the use case is highly latency tolerant.

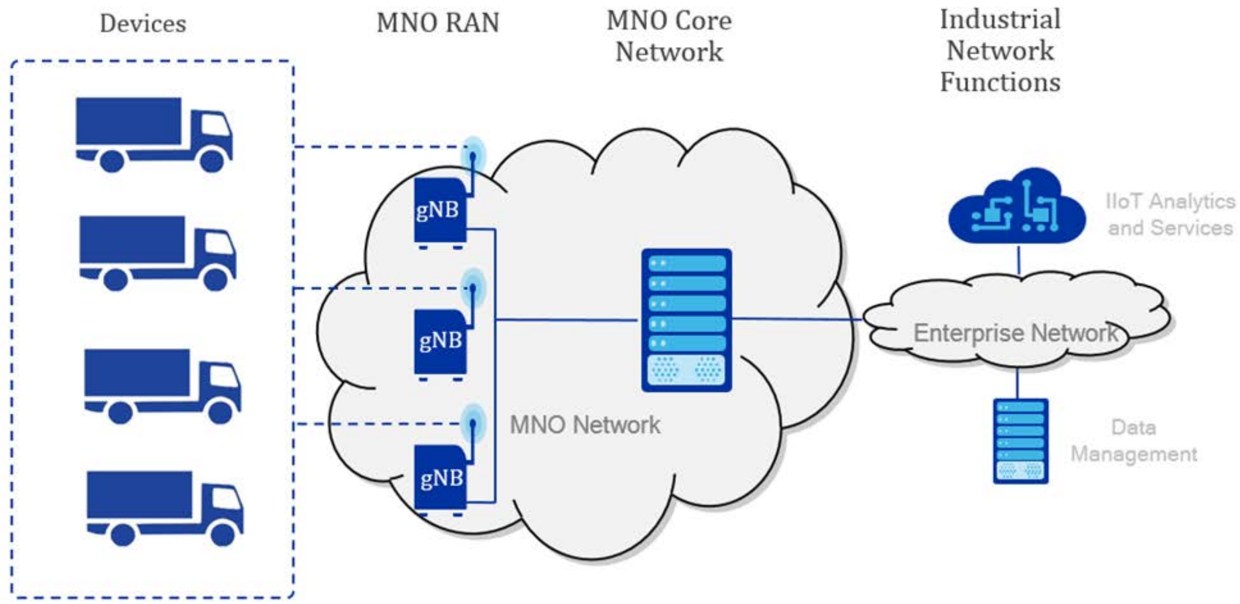


Figure 5.3. 5G for Industrial Automation.

The fleet of HGVs periodically upload telematics data via the MNO-connected connectivity modules. This upload is very delay tolerant (>30 min). The data is routed via MNO network to the HGV manufacturer's enterprise server for analytics and storage. After analysis, a new Engine Control Unit (ECU) remapping is generated for an individual HGV and is transmitted down to the vehicle for installation at a convenient time (for example, when the vehicle is parked). This installation may also be scheduled to happen live with an OTA connection (again, at a convenient time). The vehicle continues periodic telematics upload throughout. Data upload and download operates with use case-appropriate performance.

5.1.4 USE CASE 4: PROGRAM MAKING AND SPECIAL EVENTS (PMSE)

The Program Making and Special Events (PMSE) industry supports live activities at scenes—for example, program production, event/conference hosting, stage control and enhanced audience experiences for concerts, TV shows, theaters, musicals, press conferences and electronic news gathering. The devices for PMSE can be microphones, in-ear monitors, cameras, displays, projectors and other devices for handling audio and video media types. With UE capability embedded with the PMSE devices, the 5G system needs to be able to support processing audio and video data streams as well as delivering control data for remote control of wireless devices with a guaranteed quality of service in terms of latency, audio/video quality, availability and reliability of wireless links.

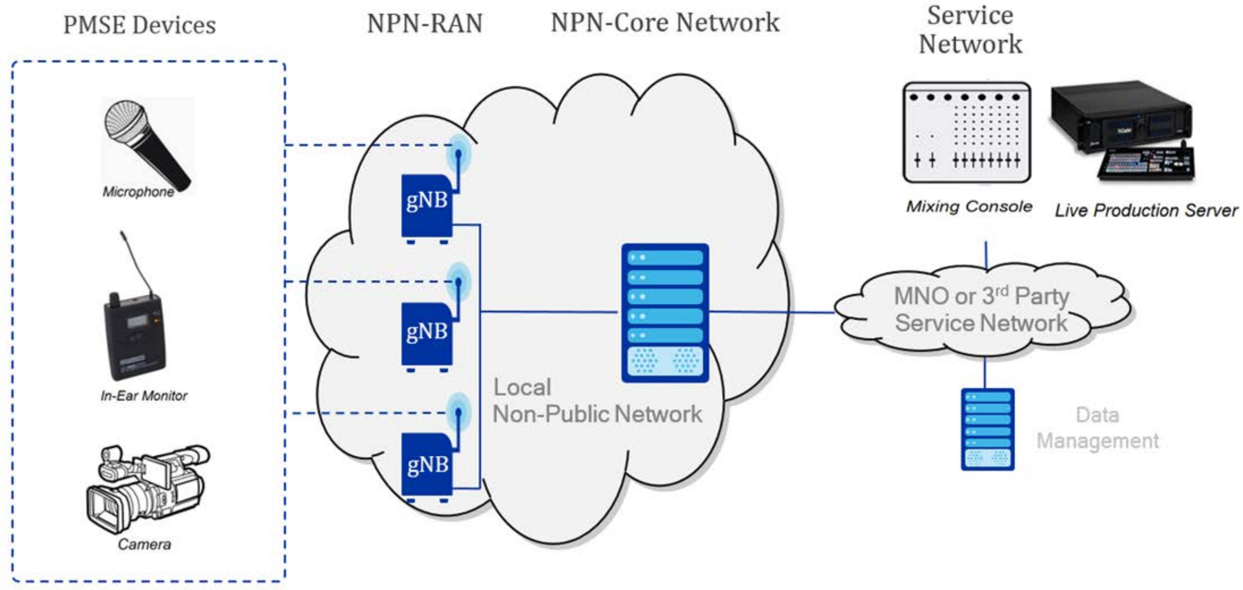


Figure 5.4. PMSE with Private Network for Live Program Production.

The major challenges for a 5G network in supporting the PMSE industry include a wide variety of deployment and security requirements for different live use cases, stringent URLLC requirements in terms of end-to-end latency, jitter, audio/video quality, synchronicity, communication service availability and reliability for a large number of wireless connections, and real-time support of continuous monitoring of the current network states for the avoidance of interruption in the middle of audio-visual (A/V) content production.

As an example of live program production for a live concert, PMSE devices such as microphones, in-ear monitors, and cameras register to the local non-public network. The local non-public network establishes a data connection for the devices and connects to mixing console and live production server in the service network, which may be operated by the MNO or a third-party network operator. The PMSE devices transmit the audio and the video to the mixing console and live production server. The mixing console and live production server process and edit the received audio and video. The output of the mixing console and live produced program can be sent back to the performers wearing the in-ear monitors or stored in the data servers for providing live streaming service to subscribed audiences.

6. SECURITY

The mobile wireless industry's long-standing emphasis on security has been a strong market differentiator against many other wireless technologies. With 5G, the mobile wireless industry takes that security focus to another level with a wide variety of new, advanced safeguards. In October of 2018, 5G Americas published a whitepaper titled The Evolution of Security in 5G.

6.1 INTRODUCTION

5G technology will support a wide range of vertical applications such as IoT, Virtual Reality (VR), industrial control, smart cities, smart grids and smart factories.[8] The Industrial IoT (IIoT) networks, enabled by 5G technology, are known to be vulnerable to different cyberattacks.[9] In the event of a successful attack on IIoT systems, there is a potential for devastating consequences. Therefore, it is critical to have security integrated into the design of IIoT networks—it should not be an afterthought. In the following sections, we describe the different threats targeting IIoT systems, the security requirements and the relevant security standards.

6.1.2 INDUSTRIAL IOT SECURITY THREATS

The cyberattacks targeting IIoT systems are evolving and are becoming more difficult to detect and mitigate against. Threat actors[10] who may target IIoT systems include, but are not limited to, the following:

- **Cyber Attackers** – The cyber attackers target IIoT systems with the objectives of monetary gains, spying, spoofing, injecting malicious malware, or launching a Distributed Denial of Service (DDoS) attack to disrupt critical services.
- **Bot-network Masters –** These actors control a large number of infected IIoT devices and use Command and Control (C&C) servers to instruct botnet members to launch DDoS attacks on operators' networks and public websites. These types of attacks are critical attacks, especially when they cause outages and unavailability of emergency services.
- **Industrial Spies and Organized Crime Groups –** International corporate spies and organized crime organizations may pose a significant threat to IIoT systems through their ability to conduct industrial espionage and large-scale monetary theft, as well as their ability to hire or develop hacker talent. Their goals are profit based, such as theft of trade secrets to gain access and blackmail the affected industry using potential public exposure as a threat.
- **Terrorist Groups** – Traditional terrorist adversaries are less developed in their computer network capabilities. Therefore, they pose only a limited cyber threat on IIoT systems. In the future, they may pose more substantial cyber threats against IIoT systems.
- **National Governments** – National cyber warfare programs are unique in posing threats ranging from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption.
- **Insiders –** Exploits from insiders can be both intentional and unintentional. While disgruntled insiders can be threat actors causing serious damage, unintentional human errors contribute to a high percentage of incidents in enterprises.

[8] 3GPP 22.261: *Service requirements for next generation new services and markets.*
[9] https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.
[10] Ibid.

Some common types of attacks on IIoT networks include the following:[11]

- Malware-triggered ransomware – Malware such as a virus, worm, or Trojan that infects the IIoT system, locks the system and demands some form of payment to unlock
- Network protocol attacks
- Cryptographic algorithm and key management attacks
- Spoofing and masquerading (authentication attacks)
- Unauthorized endpoint control to trigger unintended control flows
- Data corruption attacks
- Distributed denial of service (DDoS)
- Physical security attacks
- Access control attacks (for example, privilege escalation)

Figure 6.1 shows an example of a recent cyberattack. In 2016, hackers launched "Mirai" DDoS attacks by infecting multiple Internet-connected devices (surveillance cameras, DVRs, routers, etc.). The compromised devices were used to launch a coordinated DDoS assault on an array of targets including web hosting service providers and journalists. Launching this "Botnet of Things" attack did not require a high level of programming skills.[12]

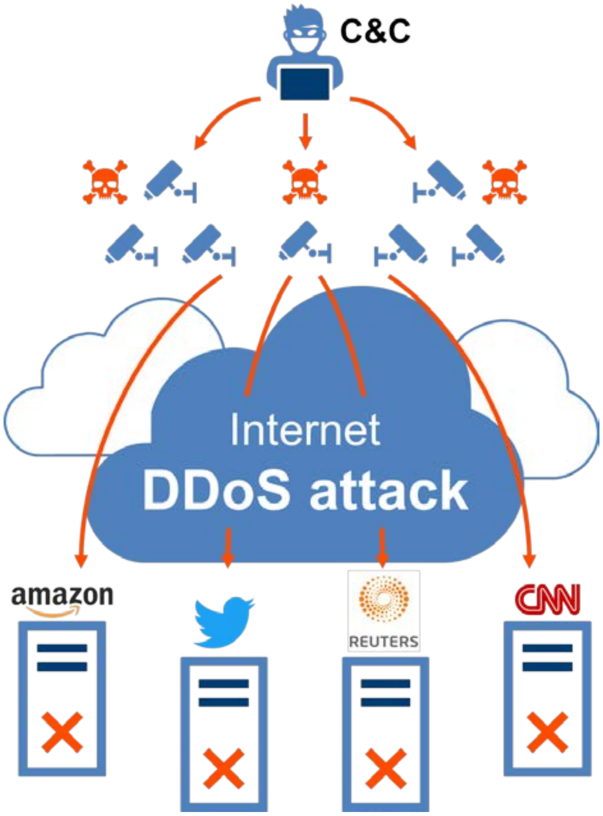


Figure 6.1. An example of IoT DDoS Attack - Mirai Attack.

[11] https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.
[12] https://en.wikipedia.org/wiki/Mirai_(malware).

A similar DDoS attack could be launched against a 5G RAN and Core network using a botnet of infected IIoT devices, which might impact the availability of operators' critical services such as emergency services.

6.2 INDUSTRIAL IOT SECURITY REQUIREMENTS AND STANDARDS

Security for IIoT networks comes with unique security priorities, management and operational characteristics and requirements. The main IIoT security objectives include the following:

- **Confidentiality:** Protecting sensitive information from disclosure and maintaining data privacy.
- **Integrity:** Information is not modified, intentionally or unintentionally, without being detected.
- **Authentication:** Data is accessed by known entities while making sure that that data belongs to the verified identity.
- **Non-repudiation:** Ensuring that an individual or system cannot deny having performed an action.
- **Availability:** Ensuring that information is available when needed. Automation systems tend to put a lot of emphasis on availability. The real-time behavior of automation systems can be critical, especially for control applications.
- **Privacy:** Protecting the data that could lead to tracking user location and monitoring user behavior and activities.

There are many cyber security standards, guidelines and regulations imposed by governments and industries that provide best practices, guidelines and requirements. Key guidelines include the following:

NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security

The NIST SP 800-82 standard document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

ISA99: Industrial Automation and Control Systems Security Standards

The ISA99[13] standards development committee brings together industrial cyber security experts from across the globe to develop ISA standards on industrial automation and control systems security. This original and ongoing ISA99 work is being utilized by the International Electrotechnical Commission in producing the multi-standard IEC 62443 series.

IEC 62443: Industrial Network and System Security

The international industrial security standard IEC 62443 is a security framework defined by the International Electrotechnical Commission (IEC). The industrial security standard IEC 62443 is applied to various vertical domains, including factory automation, process automation, building automation, transportation systems and energy management.

IEC 62443 covers both organizational and technical aspects of security and defines security requirements targeting the solution operator and the integrator, but also the product vendor. It covers the following:

[13] http://www.isa.org/isa99.

- Requirements concerning the setup of a security organization (related to information security management systems), solution suppliers and service provider processes
- Technical requirements and methodology for security at a system-wide level
- Requirements concerning the security development life cycle of system components, and security requirements for such components at a technical level

ISO 27001

ISO 27001[14] provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The objective of the standard itself is to provide requirements for establishing, implementing, maintaining and continuously improving an ISMS.

ISO 27002

ISO 27002 establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management within an organization. The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

6.2.1 INDUSTRIAL SECURITY RESPONSIBILITIES

Security in vertical use cases, in general, is a shared responsibility between a product supplier (typically, the product manufacturer), the integrator and the operator of the infrastructure.

An example illustration of these roles for the automation of an electric-power distribution grid use case is presented in Figure 6.2.

- The infrastructure operator in question is a utility
- The integrator is typically the company installing the hardware
- The Operational Technology (OT) infrastructure in question is the energy automation equipment for operating the digital grid
- The infrastructure operator is responsible for both the Information Technology (IT) and OT installation
- An example for OT is an adjustable transformer, and an example for IT is consumer and prosumer billing software
- Suppliers of automation equipment utilizing a 5G network include both electric-power distribution grid automation and 5G equipment

To address the cyber security needs of the infrastructure operator, these actors rely on adequate processes for handling IT security, as well as on technical and procedural security means. These actors thus require sufficiently secure products, but also a secure integration of products into systems and solutions.

[14] www.iso.org, www.27000.org.

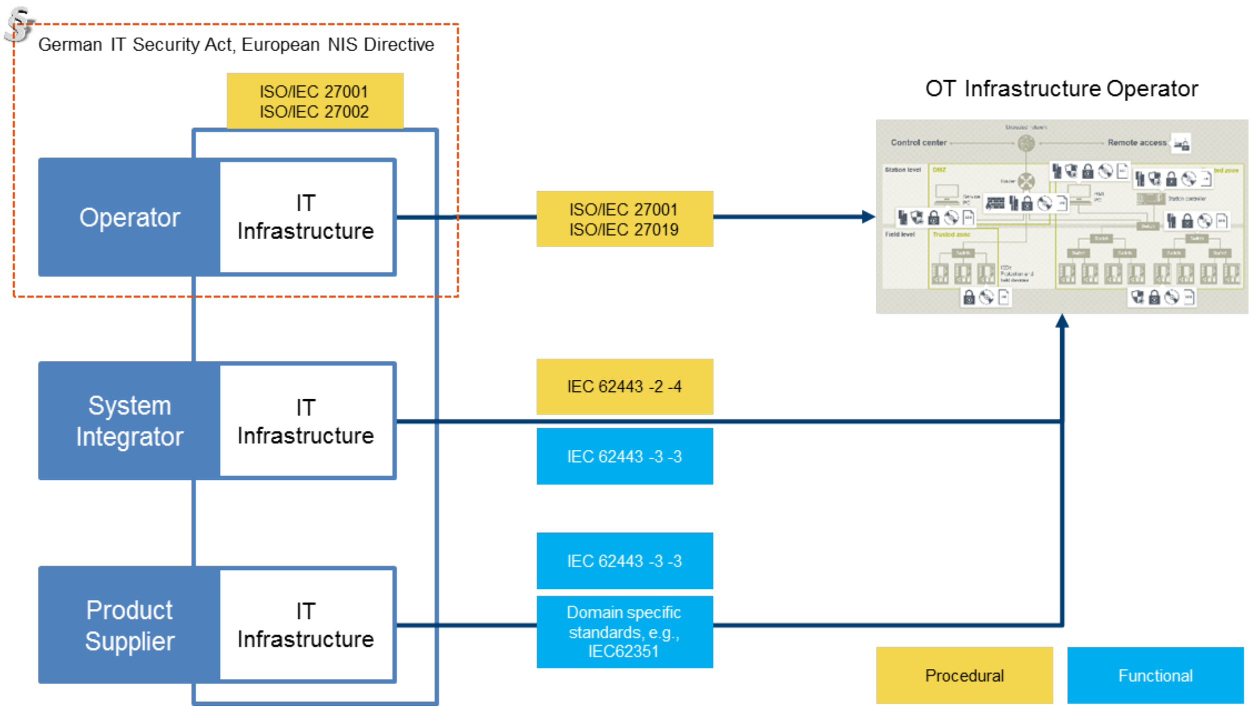


Figure 6.2. Example of Security Responsibilities in Automation in Electric-Power Distribution Grid.

Operation risks in an IT infrastructure are typically addressed with an information security management system. The ISO 27000 series defines the security management system by specifying operational processes and procedures addressing security. This framework also provides specific guidance on certain vertical domains.

Many of the processes above require interfaces, which come with requirements for the integrator and the device or system manufacturer. The integrator defines security requirements based on the intended operational use cases and determines security levels to be achieved. IEC 62443, Clause 6.3, is the defining standard.

In this context, it is also important to remember that the security mechanisms should be supported for at least the life expectancy of the installed devices. This life expectancy is typically ten years or more.

If 5G UEs are installed in a factory, for instance, the 5G system and future updates to the system have to support the initially used authentication mechanism for the same time span. Compatibility of 5G security solutions with IEC 62443 is important so that 5G offerings can be used flexibly in different industrial domains.

5G security is essential for low-latency, high-reliability communication used in automation, for example, in industrial automation, Industry 4. 0, Industrial IoT, building automation and the electric-power distribution grid.

6.3 5G SECURITY FOR AUTOMATION APPLICATIONS

Depending on how 5G networks and 5G technologies are used by a vertical automation application, different requirements have to be met by the underlying 5G security solutions.

6.3.1 QUALITY PROPERTIES OF 5G SECURITY SOLUTIONS

5G offers new and enhanced capabilities to provide secure solutions for consumer, enterprise and the growing Internet of Things.

6.3.1.1 AUTHENICATION OF COMMUNICATION PEERS AND THE 5G SYSTEM

Security responsibilities for automation in vertical domains are complex, as they are shared by several actors and need to be managed by credential pairs or certificates from different sources. Authentication and verification are implemented using the Extensible Authentication Protocol (EAP) framework. 5G security features include native support of EAP. The 5G mandate of supporting EAP Authentication and Key Agreement (EAP-AKA) allows adding new EAP authentication methods in the future that can be used for authenticating IIoT systems.

6.3.1.2 FLEXIBLE SUBSCRIBER ACCESS MANAGEMENT

Efficient management of 5G subscriptions/permissions is important for 5G UEs that provide communication among automation system entities (for example, machinery on a factory floor). In this context, management represents adding UEs to a 5G subscription so that they can use 5G communication services, but also for removing UEs from the subscription base.

Subscriber access management may involve action on the UE side, for example, installation or activation of pre-installed security credentials in the UE, as well as action at the network side, for example, enabling network access to these UEs on the factory floor.

6.3.1.3 LONG TERM SECURITY

Devices in many verticals operate over long usage periods (in industrial environments typically 10 to 20 years). It is important that an automation application system can be kept in service over a long usage period without requiring regular physical access to the devices for upgrades (for example., replacing hardware components; redesigning the technical solution).

However, it is also critical for the distributed automation application that UEs are upgradable or can be patched (including firmware, security-related algorithms, and long-term keys) to maintain the security of the system to the state-of-the-art over the life span of the devices.

6.3.1.4 5G AS COMMUNICATION INFRASTRUCTURE

When the security provided by the communication system is deemed to be insufficient for a vertical automation application, security of the industrial solution is realized on top of the application layer (for example, using Internet Protocol Security (IPsec) or Transport Layer Security (TLS)).

5G offers secure communications and state-of-the-art encryption. Integrity protection mechanisms are utilized in 5G to protect the user plane, control plane and management traffic. In addition, 5G supports user privacy protection for the information that can be used by unauthorized parties to identify and track subscribers (for example, protecting permanent identifiers such as Subscription Permanent Identifier (SUPI), International Mobile Subscriber Identity (IMSI), and International Mobile Equipment Identity (IMEI)).

6.3.1.5 5G NETWORK SLICING

A network slice,[15] namely a “5G slice,” is composed of a collection of 5G network functions and specific Radio Access Technology (RAT) settings that are combined for the specific use case or business model.

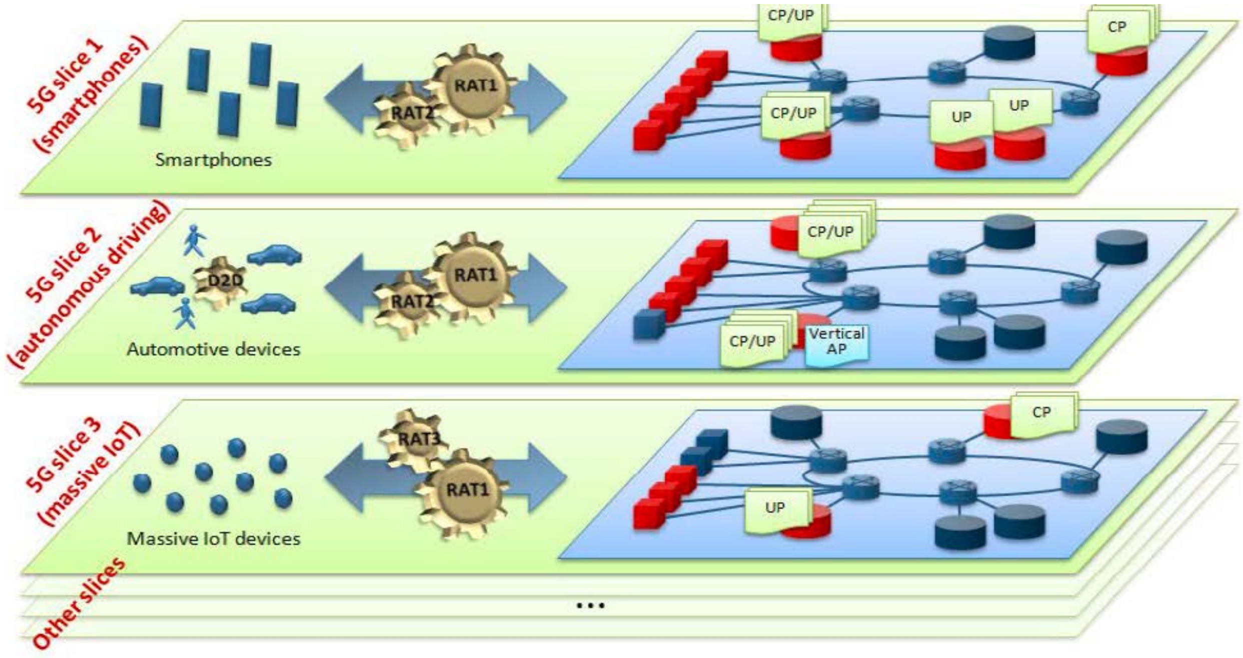


Figure 6.3. 5G Network Slices Implemented on the Same Infrastructure

A 5G slice intends to provide only the traffic treatment that is necessary for the use case and avoid all other unnecessary functionality. The flexibility behind the slice concept is a key enabler to both expand existing businesses and create new businesses. Third-party entities can be permitted to control certain aspects of slicing via a suitable API to provide tailored services.

Figure 6.3 illustrates the 5G network slicing concept, in which multiple 5G slices concurrently operate on the same infrastructure. A dedicated slice can be used for Industrial IoT, where security, reliability, and latency are optimized to meet the stringent IIoT requirements. The IIoT slice will be protected from the spread of malware that might have infected functions in another slice through slices isolation mechanisms.

[15] NGMN 5G Whitepaper, 17 February 2015,

7. 3GPP AUTOMATION DESIGN AND SPECIFICATION STATUS

3GPP has been working on the standardization of 5G mobile communication systems for the commercialization of 5G in 2020. Radio Access Network (RAN) and Service and System Aspects (SA) are the representative Technical Specification Groups (TSGs) within 3GPP. The TSG RAN is developing documents covering radio access architecture and radio interface protocol aspects of new Radio Access Technology (RAT). SA Working Group 2 (SA2), within the TSG SA, studies architecture and main functions of the 5G network system under the Next Generation system (NextGen) study item.

The SA2 finalized the NextGen Phase 1 study in December 2016 and published the 3GPP TR 23.799 specification as an outcome of the study. The NextGen Phase 2 study began in mid-2017. Based on the agreements within the NextGen study, SA2 group conducted normative standardization work for 5G mobile core network architecture and finalized the initial architecture at the end of 2017. The following subsections describe the 3GPP current efforts regarding automation design in SA1 and SA2 committees.

7.1 SA1

The 3GPP SA1 committee recognized that 5G systems would enable the extension of communication services into new, vertical application domains involving automated control. This network automation may impose demanding requirements on communication data rates, latency, reliability and availability. Each service may have a unique set of requirements, and these services may run in parallel with other less-demanding services on the same 5G infrastructure. In March of 2017, the SA1 committee started work on technical report TR 22.804, "Study on Communication for Automation in Vertical Domains," to document anticipated vertical domain use cases and identify potential 5G service requirements. Work on the technical report was completed in May of 2018.

TR 22.804 provides comprehensive documentation of use cases in the following areas:

- Rail-bound mass transit
- Building automation
- Factories of the future
- eHealth
- Smart cities
- Electrical power distribution
- Central power generation
- Program making and special events
- Smart agriculture

These use cases are used to derive potential service requirements (3GPP technical reports are non-normative, hence any requirements mentioned in them are suggestions for future, normative specifications). The service requirements fall into several categories:

- Communication requirements (availability, latency, jitter, bit rate, etcetera)
- Clock synchronization
- Positioning (availability, latency, heading accuracy, etcetera)
- Network-type support requirements
- Isolation
- Service continuity and mobility
- QoS assurance, monitoring and reporting

- Network service exposure requirements
- Security (data integrity, Denial of Service (DoS) prevention, authentication, authorization)
- Network discovery and selection

The technical report contains an introductory description of automation concepts, including activity patterns in open and closed-loop control systems, communication attributes of control systems, and communication system dependability. Security as it applies to 5G automation applications is also addressed.

Another SA1 study item, entitled "Feasibility Study on LAN Support in 5G" (work item code FS_5GLAN), was also completed in May 2018. The outcome of the study is the technical report TR 22.821, and the normative work has been started to include consolidated service requirements for 5GLAN into TS 22.261 for Rel-16 stage 1 specification. A third SA1 study item, entitled "Study on Business Role Models for Network Slicing" (work item code FS_BMNS), was completed in July 2018. The outcome of the study is the technical report TR 22.830. The normative work has been started to include consolidated service requirements into TS 22.261 for Rel-16 stage 1 specifications. The 3GPP freeze date for Rel-16 normative requirements is for December 2018. All three studies are expected to be complete by that time.

7.2 SA2

The 3GPP SA2 WG is chartered with developing the system architecture based on the service requirements elaborated by SA1. With the stage 1 study's completion in May 2018, 3GPP SA2 WG has started a new study item in stage 2, entitled "Study on 5GS Enhanced Support of Vertical and LAN Services" (study item code FS Vertical LAN), to fulfill Stage 1 service requirements in vertical domains, as defined in TS22.261 and TS22.104.

The objective of the study item in SA2 WG is to study enhancements to 5GS which can fulfil Stage 1 service requirements in vertical domains, as defined in TS22.261 and TS22.104. The enhancements to the 5G system include the following aspects:

- Support for system architecture of non-public networks, as well as the interworking and service continuity between PLMN and non-public networks
- Support for security protection to access the non-public networks, as well as the interworking between PLMN and non-public networks. The follow up study for the security mechanisms is the responsibility of 3GPP SA3 WG
- Support for new KPIs (for example, 5QI) required by the vertical service, 5GLAN type services with IP or non-IP sessions, and service exposure via APIs for third-party use of functionalities (for example, for information regarding the geographic location of coverage area of the non-public network)
- Support for the enablers of time sensitive networking (for example, time synchronization of packet delivery in each hop) and industrial control use cases specified by Stage 1

The technical report in TR 23.734, which captures the identified key issues and solutions, is expected to be completed by December 2018. The conclusions and solutions will be included in normative Technical Specification for 5GS in Rel-16.

7.3 POSSIBLE NEW IMPROVEMENTS

While the Rel-15 5G system provided a sound basis for automation communications, several areas for improvement have already been identified for Rel-16. Increased participation by verticals will help in improving the accuracy of the performance requirements discussed in TR 22.804 (Study on Communication for Automation in Vertical Domains), and it brought a wider variety of use cases and greater understanding of the deployment considerations for verticals in TR 22.804, TR 22.821 (Study on LAN Support in 5G), and TR 830 (Feasibility Study on Business Role Models for Network Slicing). As the results of these SA1 studies are now being considered for normative requirements in Rel-16, SA2 has begun to study the architectural impact of meeting these new requirements.

With the Rel-16 requirements freeze coming up in 4th quarter 2018, SA1 is now turning its sights towards further enhancements for Rel-17. Additional verticals are attending, bringing new insights into how 3GPP technology can be utilized in new industries such as streaming services, A/V production, critical medicine, asset tracking, unmanned aerial vehicles and more. While the application fields of these new studies are different from automation communication, there are similarities in the underlying system requirements needed to meet their communication needs. The Rel-17 studies will focus on identifying new requirements specific to the applications that go beyond what is already supported in Rel-15 and Rel-16.

7.3.1 CHALLENGES

A significant challenge to meeting the communications requirements for automation is the 3GPP workload. SA1 produced many requirements in the Rel-15 timeframe for IoT, automation communication, and resource efficiencies that were not fulfilled by the Rel-15 stage 2 and stage 3, which focused on eMBB. As the stage 2 and stage 3 groups are now considering those requirements, plus the additional requirements developed by SA1 for Rel-16, they are having serious discussions on prioritization to move the work forward as efficiently as possible. However, because of the prioritization exercises, not all requirements currently on the table for Rel-16 will be able to be fulfilled in stage 2 and stage 3.

Some of the KPIs identified in Rel-16 requirements will require significant radio enhancements as well as support by the core network. Several studies are underway in the 3GPP RAN groups to understand what enhancements are needed to meet the new requirements. The outcomes of those studies will determine what requirements can be met in Rel-16 and what may be deferred to Rel-17.

8. CONCLUSIONS AND RECOMMENDATIONS

5G systems will touch almost every aspect of telecom network and services. On both the access and core side, 5G use cases can be classified in terms of requirements for three essential types of communication with different objectives: massive machine-type communication, critical communications, and extreme or enhanced mobile broadband.

The ongoing development of 5G mobile communication technology will be the cornerstone to enable communications for automation in various vertical domains. 3GPP, which has developed the most successful standard technologies in the mobile communication market, such as Universal Mobile Telecommunication System (UMTS) and LTE, is currently carrying out the standardization of both 5G RAN and 5G core and expanding to features for automation implementation for use cases in various vertical domains.

It is necessary to reduce latency and connect many devices to the network while increasing the data rate to support the above services, which are the fundamental requirements for automation in vertical domains.

Industry 4.0 and the manufacturing industry, which encompasses many diverse use cases with challenging requirements that are outlined in this white paper, will greatly benefit from 5G communication technologies. Key technology building blocks and enablers of 5G systems also described in this white paper will help in the realization of 5G, the Industry 4.0 vision, and deployments where automation is a critical element.

APPENDIX A: ACRONYM LIST

3GPP	Third-Generation Partnership Project
4G	Fourth Generation cellular mobile communications
5G	Fifth Generation cellular mobile communications
A/V	Audio Video or Audiovisual
API	Application Program Interface
AI	Artificial Intelligence
B2B	Business to Business
BMS	Building Management System
BSS	Business Support Services
C & C	Command and Control
CCTV	Closed Circuit Television
cMTC	Critical Machine Type Communication
DDoS	Distributed Denial of Service
DVR	Digital Video Recorder
E2E	End to End
ECU	Engine Control Unit
eMBB	Enhanced Mobile Broadband
eNB	Evolved NodeB
ETSI	European Telecommunications Standards Institute
gNB	Next-Generation NodeB
HGV	Heavy Goods Vehicle
HVAC	Heating, Ventilation and Air Conditioning
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity
IIoT	Industrial Internet of Things
IoT	Internet of Things
MIoT	Massive Internet of Things
IEC	International Electrotechnical Commission
IPSec	Internet Protocol Security
ISA	International Society of Automation

I8SMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
LTE	Long Term Evolution
MEC	Multi-access Edge Computing
MNO	Mobile Network Operators
mMTC	Massive Machine-Type Communications
mmWave	millimeter Wave
NB-IOT	Narrowband IOT
NG-RAN	Next Generation Radio Access Network
NIST	National Institute of Standards and Technology
NR	New Radio
NTN	Non-Terrestrial Networks
OSS	Operational Support Systems
OT	Operation Technology
OTA	Over the Air
PLMN	Public Land Mobile Network
PMSE	Program-Making and Special Events
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
SA	Service & System Aspects
SA1	3GPP Specifications Group for Services
SA2	3GPP Specifications Group for Architecture
SME	Subject Matter Expert
SST	Slice/Service Types
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
TSG	Technical Specifications Group
UE	User Equipment

UMTS	Universal Mobile Telecommunication System
URLLC	Ultra-Reliable, Low-Latency Communications
UTRAN	Universal Terrestrial Radio Access Network
V2X	Vehicle to Everything
VR	Virtual Reality

ACKNOWLEDGEMENTS

The mission of 5G Americas is to advocate for and foster the advancement of 5G and the transformation of LTE networks throughout the Americas region. 5G Americas is invested in developing a connected wireless community for the many economic and social benefits this will bring to all those living in the region.

5G Americas' Board of Governors members include AT&T, Cable & Wireless, Cisco, CommScope, Ericsson, Intel, Kathrein, Mavenir, Nokia, Qualcomm Incorporated, Samsung, Shaw Communications Inc., Sprint, T-Mobile USA, Inc., Telefónica and WOM.

5G Americas would like to recognize the significant project leadership and important contributions of project leader Rao Yallapragada from Intel and Jeff Collins II from Ericsson, along with notable representatives from member companies on 5G Americas' Board of Governors who participated in the development of this white paper.

The contents of this document reflect the research, analysis, and conclusions of 5G Americas and may not necessarily represent the comprehensive opinions and individual viewpoints of each particular 5G Americas member company. 5G Americas provides this document and the information contained herein for informational purposes only, for use at your sole risk. 5G Americas assumes no responsibility for errors or omissions in this document. This document is subject to revision or removal at any time without notice. No representations or warranties (whether expressed or implied) are made by 5G Americas and 5G Americas is not liable for and hereby disclaims any direct, indirect, punitive, special, incidental, consequential, or exemplary damages arising out of or in connection with the use of this document and any information contained in this document.